WINTER 2018 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss social media discovery and important strategic legal insights and groundbreaking updates.

Legal Update for Public Content on Social Media Sites

In August 2017, German statistics company, Statista, reported social media user counts at Facebook topped two billion users. Additionally, each of the top fifteen social media applications has more than one quarter of a billion users each. Included in the top fifteen are Snapchat, Instagram, Twitter, and LinkedIn. Facebook is clearly the global leader, with approximately twenty-five percent of the planet's population among its user count. Acknowledging that sixteen million Facebook user accounts are businesses taking advantage of the app's marketing potential, the vast majority of Facebook users are there to share on an individual basis. They're sharing their lives, their likes, their loves, and their causes on the internet; and while sharing among friends may be caring, in court, internet sharing can be problematic. In this article, we look at some recent cases heard with regard to social media.

Not a Matter of Privacy

In much the same way a letter is out of the sender's control after it reaches a recipient, once information is posted on social media, there's very little that can be debated from the aspect of privacy. Whether the posting is made on Facebook or another social media app, courts have almost unanimously decided, content published on social media sites is discoverable. In fact, in a search of cases regarding social media discovery, the more current the case, the less likely it is to find a privacy-based challenge, evidencing the acceptance that social media content is discoverable.

While social media content is discoverable, requests for production of social media account information, including postings, photographs, and login credentials have been challenged on various grounds with varying rates of success. Courts are holding to the idea that social media content must meet the same standards as other material subject to discovery under applicable rules. Conversely, attempts to dishonestly thwart production of social media evidence can invalidate objections that might otherwise have limited production.

In *Crowe v. MARQUETTE TRANSPORTATION COMPANY GULF-INLAND, LLC, (Dist. Court, ED Louisiana 2015 Civil Action No. 14-1130)*, the plaintiff responded to a request to produce his Facebook history from his date of employment forward, with a refusal to produce the history, even claiming that (1) he ceased using Facebook as of 2014, and (2) when confronted with history showing he posted on Facebook after that date, he claimed the account was not his. Plaintiff later responded with the production of over 4,000 pages of Facebook account history, which the court relied upon to deem the earlier refusal justifications as inaccurate, making the entire 4,000 pages discoverable, and not subject to an objection on the basis of an overly broad request.

Relevance and Proportionality

The vast majority of courts agree that there must be a reasonable degree of relevance with regard to the claims of the case and to the respondent's social media content. In federal courts, relevance is defined by Rule 26 of the Federal Rules of Civil Procedure as, "any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be" at issue in the litigation. Good faith requests to produce relevant content supported by information gleaned from other aspects of discovery are often upheld.

In *UNITED STATES of America v. Dontavious M. BLAKE, Tara Jo Moore (No. 15-13395, United States Court of Appeals, Eleventh Circuit, 868 F.3d 960, 2017)*, Defendant Moore appealed her conviction based in-part on the denial of a motion to exclude evidence of Moore's Facebook history as overbroad, and as such, violated her Fourth Amendment rights. The appellate court disagreed, saying that the warrant, served in this case on Facebook, fell into the "good faith exception" rules to the Fourth Amendment, because the discovery of other evidence created a situation in which the government was able to reasonably obtain the social media evidence, even though the warrant may have been invalidated later. The appeals court agreed with the lower court that the evidence itself was still admissible. The warrant to Facebook, the appeals court determined, was not "so facially deficient" that an FBI officer could not have reasonably collected the evidence.

Authentication is Key

One aspect on which the courts are not allowing exceptions is authentication of social media evidence. The party wishing to introduce evidence collected from a social media site must be sure to prove that the page, post, or photograph is what they claim it to be. *THE PEOPLE OF THE STATE OF NEW YORK v. CHRIS PRICE (No. 58. Court of Appeals of New York 29 N.Y.3d 472, 2017)* demonstrates the court's commitment to authentication. Plaintiff's photographic evidence collected from the defendant's social media account allegedly depicted the defendant holding the weapon believed to be used in the commission of a crime. Plaintiff's witness testified that she, a law enforcement officer, discovered the posted photographed, recognized the defendant, and printed out the photograph. Because the officer did not offer evidence to authenticate who took or posted the photograph, or, when or where the photograph was taken, the court determined that the photograph was excludable as it was not properly authenticated.

Defining Public

While many courts have agreed with the idea that social media is equivalent to a public forum, there are limits to what constitutes a public setting. In *NATIONAL LABOR RELATIONS BOARD v. PIER SIXTY, LLC, (Nos. 15-1841-ag (L), 15-1962-ag (XAP)* United States Court of Appeals,

Second Circuit 2017), defendant, a catering company, sought to terminate an employee's protections under the National Labor Relations Act for posting vulgar comments about another of defendant's employees who worked in a supervisory capacity. In this matter, the court did not agree that the postings met the test for "opprobrious conduct," despite the fact that the post was set on Facebook as a "public" post with no restrictions as to who could see it. The court points to the fact that the post wasn't spoken in the workplace, and also considered a crucial action by the employee: he deleted the post upon discovering it was public.

> While a Facebook post may be visible to the whole world, including actual and potential customers, as Pier Sixty argues, Perez's outburst was not in the immediate presence of customers nor did it disrupt the catering event. Furthermore, Perez asserts that he mistakenly thought that his Facebook page was private and took the post down three days later, upon learning that it was publicly accessible. We thus conclude, according appropriate deference to the Board's factual findings and interpretation of the NLRA, that the Board did not err in ruling that Perez's Facebook post, although vulgar and inappropriate, was not so egregious as to exceed the NLRA's protection.

In this case, the deletion of the evidence actually helped preserve protections for the account holder, instead of opening his social media archives up to greater scrutiny which is typically the case.

Posting information on social media sites, whether vacation photos on Facebook or career and skills credentials on LinkedIn, may be fun or beneficial if it lands a coveted job offer. In the same vein, those posts can also expose public data over which the poster may unwittingly abdicate control, either as an individual or a company. If it's out there, it will be discovered.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

MASTERS CONFERENCE
Dallas, TX: February 28, 2018

THE ASU-ARKFELD 7TH ANNUAL EDISCOVERY
Phoenix, AZ: March 6-8, 2018

SECURING THE FUTURE OF THE INTERNET OF THINGS
San Francisco, CA: March 6-7, 2018

SYMPOSIUM ON SECURING THE IOT
San Francisco, CA: March 6-7, 2018

ABA TECHSHOW 2018
Chicago, IL: March 7-10, 2018

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: