DIGITAL MOUNTAIN®

FALL 2017 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 spooky innovative technologies.

Three Innovative and Somewhat Spooky Technologies Affecting Social Media Discovery

Fall is here and Halloween lurks near, so we thought it fitting to highlight three innovative social media technologies that are in their infancy and somewhat spooky—at least a lot more so than Snapchat's infamous Ghost logo. Depending on your perspective, Location-Based Social Intelligence, Facial Recognition, and Live Broadcasting could be inherently cool or creepy. Despite the perception, the potential uses and implications of these technologies may be the scariest aspects.

Location-Based Social Intelligence. This class of technology allows discovery based on geo-fencing. For example, when the tragic Las Vegas shooting occurred on October 1, 2017, the technology could have been deployed to search social media engines for communications related to this incident posted within a square mile of the Mandalay Bay hotel. This technology is primarily being used by researchers in the media, law enforcement, and the investigative community. The market for geo-fencing is served by companies such as DigitalStakeout, EchoSec, GeoFeedia, Snaptrends, and Media Sonar. GeoFeedia, headquartered in Chicago, is one of the larger players and has obtained funding of roughly $24 million. On March 13, 2017, Facebook updated its platform policies to prohibit mass surveillance on its platform by explicitly blocking developers from using data obtained to feed surveillance tools. As one might expect, much of the focus on personal privacy issues implicated by these systems originated with the A.C.L.U. lobbying social media providers to increase transparency on what data is being released through their APIs (Application Programming Interface), modify what data is being released to third party companies, and provide users with more control over their privacy settings. For now, many of the location-based social intelligence platforms have pivoted their messaging away from the term 'surveillance' and have become more focused on 'analytics' in their software solutions. Location-based social intelligence holds great promise, and as it becomes more sophisticated and widespread will affect social media discovery beyond the mere emergency response scenario envisioned above—notably, in 2016 the City of Las Vegas paid $10,800 to Snaptrends, a social media monitoring solution that came under scrutiny for its deployment as a surveillance tool.

Facial Recognition. This type of computer application is capable of identifying or verifying individuals from digital images, including video frames from live video sources, with exceptional accuracy. Often deployed in security systems, results can be compared with other biometrics such as fingerprints or iris recognition systems in confirming identity. Perhaps less intuitively, it has also become popular as a commercial identification and marketing tool. As part of systems such as Facebook, the number of sample photos of its 2 billion active users increases daily, thus building a larger pool of data, and resulting in increased accuracy on images identifying all of its users for targeted marketing. Facebook uses three threshold points as part of its algorithm and has a leg up on competitors in that with every tag, which is where friends identify each other in posted photographs, the system trains itself to be more accurate. Facial recognition embedded with Google Glass, Snapchat Spectacles, or potentially Facebook's version of the same, could identify people in a physical space and pull up a tremendous wealth of detailed information about a person's background in real-time. One commercial application is a mechanism at tradeshows or conferences for attendees to connect faster with relevant contacts; however, to date much of this technology has been deployed by governments, including assisting law enforcement with arrests and counter-terrorism efforts. As such, the implications and consequences are easy to imagine, especially in the case of the technology making false identifications when deployed for law enforcement purposes or as a biometric security mechanism (e.g., iPhone 8).

Another example of facial recognition technology is being championed by others beyond Facebook, such as FindFace in Russia. FindFace utilizes a facial recognition neural network algorithm developed by NTechLab to match faces uploaded by its users against faces in photographs published on VK, a Facebook-style social networking application based in St. Petersburg, Russia. VK has approximately 450 million active users and is one of the top 10 social media sites worldwide. The future commercial usage of these powerful and personally invasive technologies hinges on developments on privacy laws and corresponding enforcement, such as how regulators will enforce the upcoming GDPR's proclamation that biometric data (including "faceprints") is owned by the data subject and therefore requires consent before processing for particular uses.

Live Broadcasting. Facebook launched Facebook Live in 2016, enabling users to stream live video from anywhere in the world. Other companies with similar technology include YouTube (owned by Google), Periscope (owned by Twitter), and Meerkat. The technology allows musicians to remotely broadcast concerts in real-time and obtains social media input from their communities instantaneously. Unfortunately, the technology has also been used in association with crimes such as murder, rape, and robberies. Social media postings are almost impossible to claw back due to the proliferation of postings and sharing across communities within or across social media sites. Another implication of live video broadcasting is the massive amount of bandwidth consumed. Even during Mark Zuckerberg's demonstration of Facebook Live last year from his backyard in Palo Alto, he faced bandwidth constraints on his WiFi network and had to switch to broadband. Hopefully, our Internet backbone can keep up with all the taxing video demand. From the social media digital evidence perspective, video files are just another type of data to preserve for evidentiary purposes.

Whether you consider Location-Based Social Intelligence, Facial Recognition, and Live Broadcasting as spooky technologies may be a point of debate. However, there is no reasonable debate about whether social media is here to stay. Thus, to prevent our skills from ending up in the digital graveyard, it's imperative that attorneys, investigators, and litigation support professionals familiarize, utilize and embrace these technology shifts.

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

UPCOMING INDUSTRY EVENTS

Relativity Fest
Chicago, IL: October 22-25, 2017

National eDiscovery Leadership Institute
Kansas City, MO: October 30, 2017

"The Exchange" Data Privacy and Cybersecurity Forum
Washington, DC: November 1, 2017

39th Global eDiscovery Confex
San Francisco, CA: November 1, 2017

The Sedona Conference Working Group 1 Annual Meeting 2017
Phoenix, AZ: November 2-3, 2017

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: