SPRING 2019 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss the relevancy of facial recognition technology for attorneys, investigators, computer forensic examiners and data security professionals.

Biometric Data as Digital Evidence

Technology developments rapidly outpace the evolution of the law, and often for good reason. While technology advances quickly, the legal system was intentionally created to be as enduring as possible. As such, when technological advancements unforeseen by earlier courts are brought into the courtroom, trial lawyers and judges find that they are often forced to rely on precedent that isn't an exact fit. Facial recognition technology is no exception. In this article, we'll briefly review some of the Illinois Biometric Information Privacy Act, and the challenge of using facial recognition technology in legal cases.

Illinois Biometric Information Privacy Act (BIPA)

Enacted in 2008, Illinois' BIPA was the first in the nation aimed specifically at protecting the privacy of biometric identifiers, which the act defines as "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" (http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57).
BIPA requires private entities which possess biometric identifiers to:

(a) Make a written policy publicly available which includes a retention and destruction schedule;
(b) Abstain from obtaining, in any manner, biometric identifiers without informing the subject of the information that the collection is happening, why it's happening, and obtain a written release consenting to the collection, storage and use;
(c) Abstain from buying, selling, leasing, trading, or profiting from biometric identifiers without consent of the subject, or disclosure is required by law, or a proper warrant is presented compelling disclosure, or certain conditions of financial transactions make it necessary;
(d) Exercise reasonable care in protecting the privacy of biometric identifiers.

BIPA is among a small minority of privacy laws that provide for individuals to sue for violations of the act, affording a prevailing party the greater of actual damages or liquidated damages of $1,000 for negligent violations, and the greater of actual damages or $5,000 for intentional or reckless violations, as well as attorneys' fees and costs.

Under BIPA, lawsuits have been filed against Google, Facebook, Shutterfly, Six Flags Entertainment Corp., the owner of Six Flags theme parks, and many others, often by employees suing over the collection of fingerprints. *Rosenbach v. Six Flags Entm't Corp.*, (2017 Ill. App. 160317) is a notable standout among the BIPA lawsuits as the plaintiff received support from the Illinois Supreme Court for her position that under BIPA, an "aggrieved person" does not need to show actual damages, and thus, violations of the law are sufficient legal causes, as has been challenged by defendants in other cases.

Other States Following Illinois' Lead

Shortly after Illinois passed BIPA, Texas passed its own biometric privacy law in 2009. Similar to BIPA, Texas' Biometric Privacy Act differs in the areas of consent (requiring only notice), leaves the option to sue solely with the state's attorney general, and allows, under certain conditions wider than BIPA, the option to share the data (https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1357&context=ncjolt).
In 2014, Washington became the third state to pass a similar law, with more legislation pending in states such as New York, Michigan, Alaska, and Massachusetts.

California's recently passed privacy protection legislation, known as the CCPA, doesn't go into effect until January 1, 2020, so it hasn't been tested in the courts yet. The CCPA is unique in that it provides consumers with an opt-out option which prohibits the collecting entity from denying services as a result of the consumer exercising the option and has been amended to allow individuals to file suit. The CCPA also includes an expansive definition of biometric information that includes a wider array of biometrics than other states.

But Can it Win Your Court Case?

The first use of facial recognition technology as evidence in an American trial occurred in 2011, long after fingerprints and Closed-Circuit Television (CCTV) footage. There are various thoughts as to how facial recognition technology should be introduced as evidence. There is consensus, however, that the best way to handle facial recognition technology evidence is as if it were analogous to other types of evidence for which precedent already exists.

One example of this strategy is how to deal with a hearsay objection to facial recognition search results. The standard for computer-generated reports as evidence appears to be that the data generated by a computer programmed to run a specific test is not hearsay because the reports are not "statements," and computers performing the tests are not "declarants," according to *United States v. Blazier*, 69 M.J. 218, 224 (C.A.A.F. 2010). However, once human analysis is applied to the data, the testimony of the analyst is subject to cross examination, and according to Georgetown Law Technology Review's article "Machines Ascendent: Robots and the Rules of Evidence" (3 Geo. L. Tech. Rev. 1(2018)), "[e]xercising control over the machine's analysis, such as by determining what test parameters to use, renders the statement a joint statement."

Facial recognition technology isn't likely to quicken the pace by which the law adapts to modern technology. The courts have seen the introduction of enough kinds of evidence, including biometrics, that analogous forms and circumstances will not be difficult to find. However, as facial recognition technology becomes more accessible, the courts will undoubtedly see more facial recognition evidence and attorneys will have increased opportunities to include the

technology in their evidence repertoires. Staying abreast of both the technological and legal developments will help ensure that you're recognizing the best strategies and the biggest challenges you'll face in court.

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

UPCOMING INDUSTRY EVENTS

WOMEN IN EDISCOVERY NATIONAL CONFERENCE
Austin, TX: May 8-10, 2019

INTERNET OF THINGS WORLD
Santa Clara, CA: May 13-16, 2019

MASTERS CONFERENCE
Chicago, IL: May 16, 2019

TECHNO SECURITY & DIGITAL FORENSICS CONFERENCE
Myrtle Beach, SC: June 2-5, 2019

MASTERS CONFERENCE
Denver, CO: June 11, 2019

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: