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.

Facial Recognition: Increasingly Relevant for Discovery

Almost twenty years ago, the movie *Minority Report* predicted a future where billboards individually addressed consumers as they passed, stores recognized shoppers and recalled previous purchases, and cars operated autonomously. As futuristic as that sounds, all this technology already exists, and much of it thanks to facial recognition. Facial recognition technology, from both the hardware and the software perspectives, is making dramatic strides in becoming a portable part of our mainstream culture. In this article, we'll briefly review the facial recognition technology market, and then take a deeper look at how facial recognition technology is being brought into our everyday lives.

The Facial Recognition Technology Market – Big Smiles All Around

Currently, the market for facial recognition technology, including hardware, software, accessories, and service, is nearing $4 billion for 2019. Projections of the expanding market reach as high as $9 billion by the year 2023, as worldwide interest in the technology increases (https://www.marketwatch.com/press-release/facial-recognition-market-2019-global-share-trends-segmentation-analysis-and-forecast-to-2023-2019-01-04). As an easy to implement solution that has a potentially limitless number of unique subjects, facial recognition technology is used by governments and law enforcement agencies, hotels and entertainment venues, retail environments, public transportation, and banks. In addition to crime prevention, employers have a variety of choices in biometric time keeping devices, as well as computer and data security uses. Employers using facial recognition technology are able to authenticate the identity of employees by verifying that their faces were used to open a door, access data via a computer, or clock in or out of work.

Obvious Choice for Law Enforcement

In the United States, state and federal government agencies have been collecting photographs for decades, including, drivers' licenses, state identification cards, passport photographs, military identification cards, "mug shots" and "green" cards. All those documents link a physical image to identifying information. Combine all those images and information into a searchable database, add fingerprints, DNA profiles, iris patterns, and other information, and you've described the FBI's Next Generation Identification system designed to bring together as much relevant information as possible to deter and solve crimes (https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi). Collecting biometric data from multiple sources isn't new; the FBI claims to have maintained the "largest person-centric database" of fingerprints since 1999, and biometric data is often the key to solving perplexing crimes.

Companies such as NEC Corporation, IBM, and Gemalto are working with government agencies to provide facial recognition technology that can isolate faces in crowds and compare the images of those faces to databases of pre-selected images. In May 2018, the US Department of Homeland Security sponsored a test of various systems at a "rally" designed to rate the performance of twelve facial recognition and iris scanning systems using live subjects simulating travelers (https://mdtf.org/Rally2019). Interestingly, the results include a "Satisfaction" rating wherein the live participants rated their satisfaction with the tested systems, a metric which might aide the selection of screening technology currently being trialed for use in airports.

In December 2018, Delta Airlines at Atlanta's Hartsfield-Jackson Airport became the first airline to partner with the US Customs and Border Protection to use facial recognition as part of the airport security functions for international flights. Passengers flying out of Atlanta had their faces checked against the CPB's database, used the technology for check-in and baggage check, at security, and to board the plane (https://www.cbsnews.com/news/delta-americas-first-biometric-facial-recognition-airport-terminal/). The benefit to passengers is that the technology is supposed to speed up these often time-consuming processes that currently bog down travelers.

In China, the police are equipping officers with smart-glasses capable of searching the government's national identification database and rapidly returning an alert when a wanted person is located (https://www.wsj.com/articles/chinese-police-go-robocop-with-facial-recognition-glasses-1518004353). The glasses have a futuristic design similar to Google Glass, which is now only available as an enterprise version.

Voluntarily Building the Database

Over two billion Facebook users are helping the social media platform build and improve their DeepFace system by tagging friends, acquaintances, and themselves in their posted photographs. The accuracy of Facebook's facial recognition algorithm supposedly surpasses the FBI's Next Generation Identification system because the photos users tag include various poses and expressions, which helps Facebook's algorithm to create various measurements called "thresholds" that it can then use to recognize faces in a variety of formats versus the "look directly into the camera" shot that the FBI retrieves from official documents. The DeepFace algorithm accurately performs at 97.25%, which compares favorably to the human brain, known to recognize faces at high rates of accuracy in the range of 97.53%.

Facebook isn't alone in the quest for near flawless facial recognition. Google's FaceNet system was trained over one thousand hours to achieve an accuracy rate of nearly 100%. The system, when applied to user-submitted images on Google Photos, can create "clusters" of multiple images of the same face, again allowing for facial recognition to work with various poses and facial expressions. Recently, Google Photos has been presenting users with sets of two photos

and asking users to provide feedback on whether both photos are of the user, further helping to train Google's FaceNet system by refining the database.

FindFace, an app owned by Russian firm NTechLab, has stopped making its facial recognition system available to consumers after ethical and legal questions arose (https://findface.ru/). The original FindFace app was designed to allow users to snap a photo of anyone with a mobile device and submit the photo to Russian social media platform VKontakte (VK) to identify user pages matching the captured image. When it was discovered that FindFace users were publicly identifying vulnerable individuals, NTechLab redirected the app for law enforcement, security, and business users.

The enthusiasm for facial recognition technology isn't likely to decrease soon. Already ensconced in criminal investigation and prosecution, facial recognition will undoubtedly appear in civil litigation with increasing frequency – both in the discovery phase and in the courtroom as litigators use the information to test the veracity of statements, authenticate identity, and verify movement. But how close are we to billboards that address us by name? In November 2018, UK-based Bidooh won a contract to place ten thousand facial recognition equipped advertising screens in Seoul, South Korea. The future of facial recognition, it would appear, is already here.

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: