IADC COMMITTEE NEWSLETTER

CYBER SECURITY, DATA PRIVACY AND TECHNOLOGY

June 2021

IN THIS ISSUE

This piece discusses the real world benefits and pitfalls of facial recognition technology, the state of modern-day use, and the nature of the biometric data used in connection with this technology. We discuss the ethics behind the use of such data, and how security and privacy for facial recognition companies - beyond compliance currently required - can result in competitive advantage as these companies look to a future of biotechnology.

Facial Recognition Technology - The Good, Bad, and the Future

ABOUT THE AUTHORS

Avanti Bakane is a partner at Gordon, Rees, Scully, Mansukhani. As a Certified Information Privacy Professional (CIPP) and co-chair of the firm's Cyber, Privacy & Data Security group, Avanti's practice consists of representing businesses and creative professionals in software and e-commerce development, data privacy, data loss, licensing, and copyright infringement disputes. Publicly traded and smaller companies alike retain Avanti in areas such as complex class action, antitrust, breach of contract, and general commercial litigation, with a focus upon consumer class action defense. She can be reached at abakane@grsm.com.

Margaret Martin graduated from Loyola University Chicago Law School in January 2021. Margaret is licensed in Illinois, and soon to be, Washington. While in law school, Margaret spearheaded a Pro Bono Committee determined to help the underserved population mainly in areas of Domestic Violence and Expungement. Margaret's main passion is data privacy and protection, and she works in this space, for a major telecommunications company.

Kyla Guru is 18 years old and the Founder/CEO of Bits N' Bytes Cybersecurity Education, a 501(c)(3) dedicated to educating and equipping all vulnerable populations with the cybersecurity education and awareness needed to face our future of advanced cyberthreats. For the past five years, Kyla has led her organization in distributing curriculum to 500+ schools and fostered partnerships with school districts, corporations like Facebook, Verizon Media, & IBM, and educational organizations like ISACA's One in Tech in order to spark international dialogue about security.

ABOUT THE COMMITTEE

Corporations and law firms around the world are constantly dealing with cybersecurity, data privacy and other important technology issues, both in business and, where available, in litigation discovery. Burgeoning technologies are placing new and increasing demands on in house and outside lawyers and their clients. All are being challenged to meet new and strict data privacy and security guidelines and the consequences for failing to meet these requirements can be devastating. The Cyber Security, Data Privacy and Technology Committee will address the differing substantive laws globally in these areas, and be of interest to many other committees whose members and activities are impacted by technology. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

Avanti D. Bakane
Vice Chair of Publications
Gordon & Rees, LLP
abakane@grsm.com

<u>Advocates and Privacy Concerns</u>

The demands of a post COVID-19 world are causing developers of facial recognition technology to balance innovation with growing privacy concerns.

In some sectors, the pandemic has offered opportunities to refine facial recognition technology and new potential use cases. For example, the Department of Homeland Security has been in talks to deploy new algorithms to identify subjects wearing masks. A few years ago, the San Jose Airport deployed facial recognition technology to verify passport photos with its holders, easing verification lines and effectively automating the process.[1]

Other industries are seeing benefits from facial recognition technology as well. Take the banking industry, City Bank of Florida and JPMorgan Chase, for example. Long gone are the days of forgotten and compromised passwords and passcodes. Logging into your bank account using a biometric scan of your unique face now takes a few seconds.[2] Utilizing facial recognition technology not only increases expediency, but provides additional security. Prior to facial recognition software, if a theft occurred, investigations were slowed because they would have to wait for the card to be utilized. Now however, with facial recognition technology when theft occurs at an ATM, the bank has a real-time photo of the theft occurring and can locate the suspect before potential damage to the victim occurs.

However, facial recognition technology has also been widely criticized by privacy advocates for potential misuse. Facial recognition technology is not without faults. One such glaring fault is the bias the system has for people of color. In a study conducted by two MIT students called Gender Shades, the facial recognition systems were better at detecting light-skinned males; women and people of color contained more error rates.[3] With facial recognition software skewed against people of color, utilizing such technology in police investigations should raise red flags. With no federal regulations in place to limit or standardize the use of such facial recognition technology, the risk of law enforcement using technology that is biased towards a large subsect of the human population can lead to massive ethical ramifications. When facial recognition software is utilized, a human component must be present to ensure accuracy.

Just last year, Congress tried to standardize facial recognition technology under the Facial Recognition and Biometric Technology Moratorium Act of 2020. The bill did not make it past the Senate. HR 7356 does provide a preview of what federal lawmakers are considering when it comes to limiting use of facial recognition technology

[1] How San Jose Airport uses facial recognition to speed lines (sfgate.com)

[2] *See e.g.* https://www.fintechfutures.com/2018/05/hsbc-unveils-facial-recognition-banking-for-corporate-customers/

[3] http://gendershades.org/overview.html

in the future. If passed, the Act would have limited the use of face recognition, prevented federal funds from being used to purchase such technology, and stopped continued federal funding for use by law enforcement.

Varying Approaches to Limitations

With the potential scrutiny facial recognition technology brings, city leaders have taken a cautious approach to the technology, limiting its uses for specific purposes.

While many city leaders have imposed limitations on facial recognition technology, Portland leaders have taken a drastic approach, making the city the first to ban certain use of this technology by private businesses.[4] The ban prohibits private entities from using facial recognition technology in places of public accommodations, including hotels, restaurants, retail stores and public gathering locations. This would include businesses that serve the public - grocery stores and restaurants, by way of example.
Portland joins other cities like San Francisco, Oakland, and Boston that outlaw use of surveillance technology.

How Much is your Identity Worth?

The inherent value of facial recognition data makes it an attractive target for data theft and cybersecurity incidents. When evaluating the economics of this exchange, as with many industries with high-value data, incentives for malicious cyber threat actors are ever-present, with the reward for attack greatly outweighing its risks.

One of the largest motives for attackers in the healthcare sector is the resale of health information on the dark web--an average person’s identity, or “Fullz,” is “worth” $1,170 on the dark web. Specifically, data associated with facial recognition may include sensitive images, as well as “metadata,” associated with the images, including PHI like name, address, height, and/or weight.

Compared to credit card information, which can be easily replaced and closely monitored for suspicious activity, this type of health information is permanent and thus, valued at a price 10 times higher than credit card information, selling at about $360-$1,000 on the black market. The threat actor can also utilize such information for medical identity theft, larger phishing or scamming schemes, and financial fraud.

Additionally, the time-sensitivity of inaccessible healthcare information makes it a prime target for high-price ransomware attacks. Given that organizations working with facial recognition are working in critical industries like health and law enforcement, these organizations are at an elevated level of threat to ransomware attacks that could temporarily halt operations and carry grave recuperative costs. In fact, the healthcare

[4] Portland passes broadest facial recognition ban in the US - CNN

industry is the most targeted sector for ransomware attacks. As downtime and data exfiltration in the healthcare industry can be wildly detrimental to patient outcomes, companies are more apt to pay.[5]

Additionally, as a result of COVID-19, the healthcare industry saw ransomware attacks double from July to September 2020 as virtual healthcare became the norm.[6] Particularly for smaller companies, these types of ransomware attacks have disproportionately greater impact, and for a healthcare company working in AI (often associated with facial recognition), a ransomware or cyber-attack can ultimately postpone a clinical trial and cost millions of dollars as a result of the delay. Specifically, delays in clinical trials are valued at a loss of $600,000 to $8 million in future revenue per day[7], and reputational damage can have lasting business impact.

That a data breach on a facial recognition organization has wide-reaching effects on the personal privacy of citizens cannot be understated. For instance, in February 2020, Clearview Artificial Intelligence announced a data breach on their internal systems, which exposed their client list, including several law enforcement agencies. While Clearview AI denied that the adversaries had access to the over three billion photos in their database, the potential impact of intrusion of facial recognition companies is important to consider. Once inside the corporate network, privilege escalation can allow adversaries to gain access to domain accounts and images can be altered without authorization. This has been seen before in a seemingly "doomsday-esque" example, where researchers deployed malware to gain the ability to add tumors to CT or MRI scans inside of health clinics.[8]

Given the risks facing the companies positioned in the facial recognition sector, maintaining the privacy of citizens' data and the security of artificial intelligence software utilized is a bare minimum. As technology rapidly advances, this balance is proving exceedingly difficult to achieve.

For instance, DTC Genetic Testing companies also work with law enforcement, but are not subject to HIPAA despite that they possess and sell the most sensitive personal information to third parties. While genetic code is arguably at the top of information deemed unique and sensitive, the level of security required from private organizations is not parallel. Furthermore, HIPAA does not require encryption of data during the transmission of data from one party to another (third-party), which places private user information at even greater risk. Simply put, "check the box" security requirements will no longer suffice.

[5] https://purplesec.us/resources/cyber-security-statistics/#:~:text=Intellectual%20property%2049%25,Financial%20information%2026%25

[6] https://www.checkpoint.com/

[7] https://www.gopraxis.com/real-cost-clinical-trials/

[8] https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/

Steps Towards Striking a Balance

A prioritization of asset-based cybersecurity of facial recognition companies is critical. The sensitivity of data assets associated with organizations working in artificial intelligence related to digital health, as well as the prolonged reputational and regulatory impact that follow are X factors that reinforce this idea. As demonstrated above, the existing regulatory feedback mechanisms that are currently in place only represent the bare minimum for organizations to follow, particularly for agile organizations advancing in the artificial intelligence space.

This sector must focus efforts on bolstering security beyond compliance - through continual partnership between private cybersecurity companies, users of facial recognition data, and security engineers - to stay on the cutting edge. When we achieve this, security can be harnessed as a competitive advantage for AI companies in the facial recognition space and beyond.

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

MAY 2021
The Ransomware Scourge: Connectivity and Vulnerability in an Internet of Things, 5G World
David Patrón

FEBRUARY 2021
If you Want to Stay Friends with your IT Supplier, Use the Contract!
Anna Cook and Robert Graham

MARCH 2018
First Class Action Data Breach in the UK – Employer Found Vicariously Liable for Rogue Employee's Actions
Elena Jelmini Cellerini and Vikram Khurana

NOVEMBER 2017
Blockchain Unchained: One Lawyer's Quest to Figure out what the Hell Everyone is Talking About
Kendall Harrison

AUGUST 2017
Def Con Hacker Conference: An Accidental Tourists Observations
Elizabeth S. Fitch

MAY 2017
Doe v. Backpage.com and its Aftermath: Continued Uncertainty and New Litigation in the Wake of the Supreme Court's Denial of Certiorari
David Patrón

APRIL 2017
Incorporating Technology into the Management of the Work Processes at the Firm
Donna L. Burden, Elizabeth S. Fitch and Park L. Priest

FEBRUARY 2017
"The First Thing We Do, Let's Kill All The Lawyers"
Elizabeth S. Fitch and Elizabeth Haecker Ryan

DECEMBER 2016
A Primer for Understanding Blockchain
Doug Vaughn and Anna Outzen

AUGUST 2016
The Attorney-Client Relationship in the Electronic Age
Elizabeth S. Fitch and Theodore M. Schaer