Lowndes

Insights

Facial Recognition: What You Need to Know Now

Article
07.15.2020

Related Attorneys

Melody B. Lynch

If you are like me and recently purchased new technology to help you efficiently work remotely during the COVID-19 pandemic, you may be using a device that incorporates facial recognition technology into its cadre of features. While it may be more convenient than fingertip or password technology, do you really know what facial recognition technology is, why you should be concerned about it, and what corrective action can you take if your unique facial signature is improperly acquired or used without your permission by a third party?

What is facial recognition technology?

Facial recognition is a technology that maps your facial features by using biometric identifiers that are stored as hashes to create unique facial signatures. This is how your new password-protected iPad can be unlocked by simply looking at it.

Companies like Apple use facial recognition technology to authenticate their users. Apple uses its True-Depth camera system to map the geometry of your face by analyzing over 30,000 individual data points to create your unique facial signature.

Why should you be concerned?

While you may be comfortable with facial recognition technology as an acceptable tool for authentication of a particular user, the technology is being used far beyond this the realm of authentication.

Earlier this year, Clearview AI, through its founder, Hoan Ton-That, received national and international attention after it collected billions of images that it claimed were publicly available on social media and other websites under the auspices that it was aiding law enforcement in the detection and prosecution of criminals. Clearview AI scraped images from Facebook, Instagram, LinkedIn, Venmo, and other websites alleging that it had a First Amendment right to use public data. Facebook and other social media companies disagreed, citing their respective terms of service which bar such activity.

Moreover, while legitimate law enforcement purposes may exist, racial and gender bias (among other significant problems) are known to exist with facial recognition technology. Studies have shown that facial recognition technology identifies white male faces better than black male faces. The technology also identifies male faces better than female ones.

In response to these ethical concerns, major companies such as Amazon and IBM (as well as the European Union's Data Protection Board) have stepped up and either discontinued or implemented new restrictions on the use of facial recognition strategies and technologies in their companies until the technology can be honed and the guidance can be developed to ensure that it will be applied justly and fairly to all people with adequate safeguards.

According to The New York Times, facial recognition technology from companies like Clearview AI is already used by the Federal Bureau of Investigation, United States Department of Homeland Security and over 600 law enforcement agencies (including some in Florida). Once Clearview AI scrapes images from public sites, it use algorithms to compare the images against thousands of biometric identifiers to find matches. What if your image is one of the more than 3 billion images collected by Clearview AI without your knowledge or consent?

What can you do about it?

If your or your company's data is scraped, collected and utilized without your permission by third parties, you may have legal causes of action and remedies against Clearview AI or other companies who utilize facial recognition technology. In addition to state or common law claims that may be applicable to your individual situation, the Computer Fraud and Abuse Act (CFAA) may be utilized as a cause of action to collect damages against companies or individuals who scrape data which violates the website's terms of service because such access and use is "without authorization" as defined in the CFAA.

In addition, Illinois passed the Biometric Information Privacy Act (BIPA) which imposes requirements on companies that collect or obtain biometric information. While not generally applicable in Florida, it may be the wave of the future for privacy litigation. If you are a company that uses or collects this type of information and have customers or employees who are Illinois residents, then you should be cognizant of the BIPA and its application to the biometric information you have stored.

Further, if your company is looking to expand its authentication offerings to include facial recognition technology, you should contact a lawyer to discuss the advantages and disadvantages to implementation at this time. Facial recognition technology is a powerful tool that can be attractive to consumers but there are a number of pitfalls and challenges that require significant thought before implementation.

If you need advice about facial recognition technology or any other technology-related legal matter, please contact Melody B. Lynch at 407-418-6447 or melody.lynch@lowndes-law.com or any other member of our Cybersecurity, Privacy, and eDiscovery Practice Group. For more technology-related updates, please visit our Lowndes Tech blog.