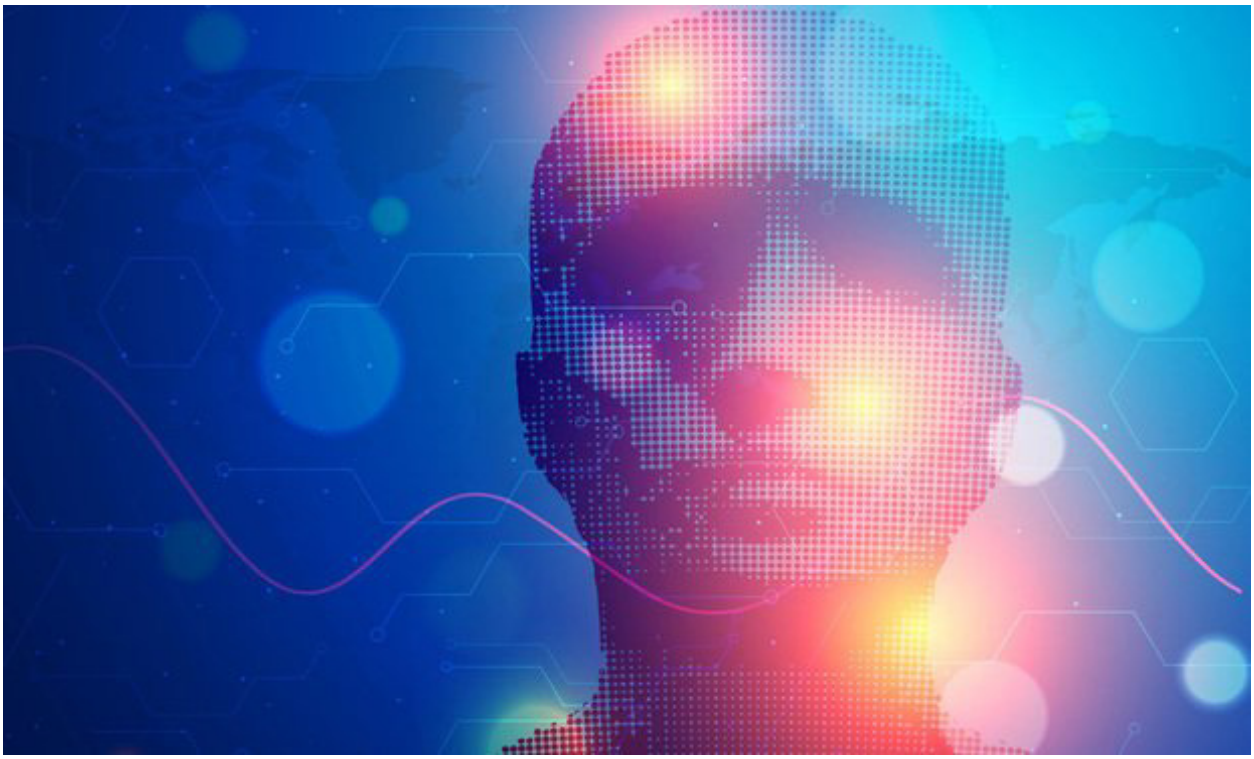
Legaltech news

Just How Scared of FaceApp Should You Be?

Biometric recognition systems like these offer an easy way to log in to our devices and various services without the hassle of typing in a series of numbers. But biometric data presents unique risks and could have far-reaching consequences if not adequately protected.

by **Brian Schrader** | January 09, 2020



No one likes typing their password, especially those long and complex ones most secure systems require today. So, when fingerprint and face ID became standard on portable devices in recent years, many of us eagerly embraced the new technology and didn't look back. Their use has expanded into the workplace

continued next page

as well, with many employers **requiring employee fingerprints** for things like clocking in and out or gaining access to a factory floor.

Biometric recognition systems like these offer an easy way to log in to our devices and various services without the hassle of typing in a series of numbers. The uniqueness of our faces, fingerprints and retinas makes them perfectly suited for quickly and accurately verifying our identities using this technology.

However, as biometric recognition systems become increasingly common, some data security experts have cautioned that the use of biometric data presents unique risks and could have far-reaching consequences if not adequately protected. Unlike passwords, we can't change our physical aspects if that data were somehow to be captured by an ill-intentioned party.

Increased Potential for Abuse

In my field of **e-discovery**, facial recognition software is being touted as a potential tool for attorneys and litigation support specialists. For example, one **new AI-based product** allows users to search through data using not just keywords but faces and objects too—potentially helping make new connections between seemingly unrelated data. Yet, as biometric technology appears in more and more settings, the potential for abuse becomes a very real concern. In **one recent case**, FBI and ICE agents were discovered to be using similar AI-based technology to scan state driver's license databases, analyzing the photos of millions of Americans without their knowledge or consent.

Several states are responding with the introduction of biometric data privacy laws, which are creating a patchwork of varying data privacy regulations across the country. The state with the strictest such law is Illinois, which in 2008 enacted the **Biometric Information Privacy Act (BIPA)**. Under this law, employers and other private entities are required to give notice to employees, get their written consent and disclose other information to them before collecting or storing their biometric data. In addition, companies collecting biometric data must create a written policy outlining how long they plan to retain the data and how they'll permanently destroy it.

A 2019 landmark decision by the Illinois Supreme Court, Rosenbach v. Six Flags Entertainment Corp., upheld consumers' right to sue companies for collecting their fingerprints without explicit consent. More than 100 class-action lawsuits had been

continued next page

filed against Six Flags after the company installed a FastPass system that utilized a fingerprint scanner, then kept customers' fingerprints on file without their full knowledge or explicit permission.

That lawsuit opened the door to companies like Six Flags potentially having to pay statutory damages to plaintiffs for violating privacy rights even when there was **no actual harm** or damage sustained. Since then, there has been a **flood of lawsuits** from employees asserting that their employers collected their biometric data without telling them how it would be used or stored.

A Puzzle with Two Pieces

As things stand right now, biometric data remains a lot more secure than a password for one simple reason: to hack into a biometric system, you need both the biometric scanner and the person using it. For personal devices, biometric data is **encrypted on the device itself** and not uploaded to the cloud, so one piece of the puzzle is useless without the other. Scanning technology has gotten accurate enough that it's difficult—not impossible, but difficult—to substitute anything for the real thing.

And let's face it—by and large, criminals are not industrious people. In fact, they're often pretty lazy. So, unless you're targeting high-net worth individuals, celebrities or other such narrow targets, the risk/reward of hacking into one person's phone is often just not worth the effort. However, as private companies and governmental agencies continue to accumulate their own **large troves of biometric data**, the risk of unsecured data falling into the wrong hands gets greater and greater.

By itself, biometric data is of limited value. Its primary use is to help gain access to something else that is truly sensitive, such as a person's Social Security and credit card numbers or a company's precious internal data. Although hackers aren't out there right now wreaking havoc with people's biometric data, the fact is, nobody knows how this technology will develop in the future. The actual effects of our biometric data getting out into the world are still somewhat esoteric and unknown, which is the truly concerning point.

The Wild West of Data Privacy Laws

Today we are in the Wild West when it comes to data privacy laws. There's a general acknowledgement that we've been too lax about protecting data privacy in

continued next page

the past, especially through the use of Facebook and other social media platforms. The unchangeable nature of biometric data does mean that we should be extremely mindful of protecting it, especially given that the use of the technology has increased exponentially.

Yet, we also have to be careful not to overregulate in a way that stifles innovation or prevents this technology from being used effectively. If a company like Six Flags faces the possibility of paying statutory damages in the millions of dollars for violating a statute, it's going to be less likely to embrace this new technology, hurting the company, its employees and its customers.

It's good that our state legislatures are attempting to address the issue now, but ultimately what we need is a set of nationwide data privacy laws similar to those of the European Union, which implemented its **General Data Protection Regulation (GDPR)** in 2018. In the meantime, all we can do is limit our use of biometric systems to the extent that we can. If our employer requires the use of biometric data, we're **well within our rights** to inquire about where our data is being stored and if the business is aware of any relevant compliance requirements. This type of vigilance has its benefits, for as the saying goes, you can't close the barn door after the horse has bolted.

*Brian Schrader, Esq., is President & CEO of BIA (**www.biaprotect.com**), a leader in reliable, innovative and cost-effective eDiscovery services. With early career experience in information management, computer technology and the law, Brian co-founded BIA in 2002 and has since developed the firm's reputation as an industry pioneer and a trusted partner for corporations and law firms around the world. He can be reached at **bschrader@biaprotect.com**.*