Lowenstein Sandler

Privacy & Cybersecurity

January 6, 2021

LET'S FACE IT: Facial Recognition Technology Involves More Than Meets the Eye

Companies considering facial recognition technology must weigh benefits against possible civil rights and privacy risks

By Mary J. Hildebrand CIPP/US/E, Diane Moss, and Manali Joglekar CIPP/US/E

The biometric data industry is growing rapidly, with the global facial recognition market alone expected to generate a tantalizing $7 billion of revenue by 2024.[1] While tech giants like Apple, Samsung, Amazon, and Microsoft have helped fuel advancements, startups and small-to-midsize tech companies also play a strong role. Lucrative contracts abound–but so do the social and legal issues. The use of facial recognition technology, and its impact on privacy and civil rights, must be weighed against its practical functionality, convenience, and profitability.

If you are a startup technology company, you may be tempted by the prospect of lucrative contracts in this area. If you are the chief technology officer of a large company, you may be seeking ways to streamline processes in healthcare or HR, for example. Whether you are producing facial recognition software or purchasing it, you need to be aware of the concomitant risks and evolving laws governing this rapidly evolving technology. In the past year and in the U.S. alone, growing allegations of race-related differences in identification accuracy rates; concerns about surveillance, civil rights abuses, and high-level security breaches; the rise of class-action privacy lawsuits; and the expansion of biometric privacy protection laws have all made headlines.[2] Like the industry itself, these concerns are global, especially as governments turn to biometric data for an ever-widening array of services. In many developing countries, facial recognition has become required in registering for healthcare, welfare assistance, food allowances, and employment. Governments are increasingly using biometric data for everything from combatting identity fraud to voting systems to monitoring social protests, and the purchase and use of biometric technology from foreign countries and private companies have raised additional alarms about the ownership and use of data.[3]

Concerns surrounding biometric data will influence both legal and industry trends. As the dynamic facial recognition industry takes us into uncharted territory, we must address the social and legal issues and wrestle with the benefits that technological advances provide, on the one hand, and their impact on privacy and society on the other.

Below is an outline of U.S. law governing facial recognition as well as a summary of some best practices for those businesses seeking to provide or use biometric data.

U.S. Laws Governing Facial Recognition

In the U.S., there is no specific federal law relating to facial recognition. However, Section 5 of the Federal Trade Commission (FTC) Act[4] gives FTC the authority to bring enforcement actions against commercial institutions that participate in unfair or deceptive trade practices relating to biometric data. Prior to 2018, Illinois, Texas, and Washington were the only

[1] https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition
[2] https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020
[3] https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html; https://www.usnews.com/news/best-countries/articles/2019-07-26/growing-number-of-countries-employing-facial-recognition-technology
[4] 15 U.S.C. §§ 45(a)(1)-(2).

three states to have biometric privacy laws. However, over the past few years, that number has increased rapidly as more and more states seek to protect and regulate collection, use, and processing of biometric data.

The Illinois Biometric Information Privacy Act (BIPA) enacted in 2008 is the first and oldest biometrics law in the U.S. that provides for a private right of action. The Texas Capture or Use of Biometric Identifier Act (CUBI)[5] follows on the footsteps of BIPA but does not provide for a private right of action. Washington's biometrics law[6] went into effect in 2017 and regulates the way iwent into effect in 2017 and regulates the way individuals and businesses can collect, store, and use biometric identifiers. This law also does not provide for a private right of action.

Since the enactment of BIPA, there has been an explosion in class action litigation under the statute in Illinois. BIPA cases have targeted employers, retailers, and online services providers. S.B. 3053, a proposed amendment to BIPA, would exempt private entities from liability under the statute if their use of the biometric information was for employment, human resources, fraud prevention, or security purposes. This amendment could significantly reduce the current wave of BIPA litigation.

Best Practices

- When deciding which facial recognition technology to use, always look for facial recognition technology provided by a third-party provider with adequate experience, certifications, monitoring, and security measures.
- If facial recognition data is compromised, it will always be compromised. Therefore, it is very important to make sure that facial recognition data is not stored with other personal information so that if facial recognition data is compromised, it will be useless without a way to tie it back to a specific individual. Best practice is to always encrypt facial recognition data while it is at rest and in transit.
- Implement appropriate policies and procedures with respect to collection, use, sharing, and processing of facial recognition data with the aim to strike a balance between security, personal privacy, and public safety.

Navigating the ecosystem of providing and using biometric data such as facial recognition tools requires utmost transparency to limit risk. Make sure you understand the data that flows in and out of your business by conducting data mapping for your company. If you are a consumer-facing business, provide accurate notices and policies regarding your collection, use, and sharing practices. Lastly, if you have not done it at all or recently, conduct a full privacy assessment and audit. For more information, contact a member of Lowenstein Sandler's Privacy Team: **Mary J. Hildebrand**, Founder and Chair of Privacy & Cybersecurity Group; **Diane Moss**, Counsel; and **Manali Joglekar**, Counsel.

About Us

In today's digital world, where data has become a key asset for conducting business, companies continue to face greater privacy and cybersecurity challenges. At Lowenstein Sandler, our Privacy & Cybersecurity team helps clients navigate the rapidly evolving, increasingly complex privacy and security law landscape in the United States, the EU, and around the world. We deliver innovative privacy and security solutions that meet our clients' critical business needs including the commercialization of data assets in a legally compliant manner. Our targeted counsel is relevant to companies across diverse industry sectors, and public and private companies from start-ups to global enterprises.

---

[5] Tex. Bus. & Com. Code Ann. § 503.001
[6] Wash. Rev. Code §§ 19.375 and 19.86

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

MARY J. HILDEBRAND CIPP/US/E
Partner
Chair, Privacy & Cybersecurity
T: 973.597.6308
mhildebrand@lowenstein.com

DIANE MOSS
Counsel
T: 973.597.2448 / 212.262.6700
dmoss@lowenstein.com

MANALI JOGLEKAR CIPP/US/E
Counsel
T: 973.597.2540
mjoglekar@lowenstein.com