Creators in film, television, music, and gaming are increasingly turning to artificial intelligence and machine learning (AI/ML) models to deliver new content and experiences to audiences. Recent headlines have highlighted these new applications, including:

- Generating music featuring imitations of headlining artists' voices.
- Creating content featuring AI-generated representations of actors' voices and likenesses.
- Creating personalized gaming avatars or characters from "selfies."
- Translating content into foreign languages using the speaker's own voice.

Depending on their particular nature, some applications of AI/ML in these and other contexts could potentially trigger biometric privacy laws.

Various states and even the federal government have considered enacting or have enacted biometric privacy legislation. Most notably, the Illinois Biometric Privacy Act (BIPA) and the Texas Capture or Use of Biometric Identifier law (CUBI) regulate the collection, use, and disclosure of biometric data. These laws regulate "biometric identifiers," a term that includes retina or iris scans, fingerprints, voiceprints, and "scans" (BIPA) or "records" (CUBI) of hand or face geometry. BIPA also regulates "biometric information," which is information based on a biometric identifier used to identify a specific individual. Under these laws, businesses that collect biometric data may need to comply with notice and consent requirements, limitations on sharing, limitations on retention, and data security requirements, among others. Importantly, BIPA permits private parties to sue for violations and has generated thousands of class actions. Beyond these biometric-specific laws, general state privacy laws also include requirements regarding "sensitive" personal data, which can include biometric data.

Because of the potential risks associated with biometric data, entities utilizing AI/ML models should consider the following issues:

- **Does the AI/ML model collect biometric data?** Although the definition of what constitutes "biometric" data varies from jurisdiction to jurisdiction, AI/ML technologies that measure, scan, or analyze a person's hands, face, eyes, or other physical features could potentially involve collecting or using biometric data. Technologies that analyze, duplicate, or create "voiceprints" could also potentially involve such data. Because the definition of biometric data is jurisdiction- and fact-specific, creators using AI/ML models should obtain advice from experienced biometric privacy counsel to determine whether biometric data is being collected.
- **What data sets were used to train the AI/ML model?** Beyond analyzing how the relevant AI/ML model works, consider how the model was trained. In some cases, training AI/ML models using images and videos could arguably trigger biometric privacy laws. Training AI/ML models using improperly obtained data sets could, in some cases, expose creators to the drastic remedy of "algorithmic disgorgement," requiring destruction of the models (and potentially the content generated from those models).
- **Is notice or consent required?** Some jurisdictions may require a business to give notice and obtain consent before collecting, processing, or sharing biometric data. These laws may be triggered in some cases even if the data is processed quickly and immediately discarded. The specific language to provide notice and obtain consent must be carefully crafted to comply with applicable law.
- **Are there limits on retention?** Some jurisdictions limit how long a business may retain biometric data. These time limitations are often tied to the expiration of the purpose for which the biometric data was collected. BIPA also requires companies to publish retention and deletion schedules. Accordingly, businesses must carefully craft their retention and deletion policies as applied to biometric data.
- **Are there limits on profiting?** Some jurisdictions also limit the ability to sell, lease, trade, or otherwise profit from biometric data. This issue may require a nuanced analysis of the use and disclosure of biometric data.
- **Are appropriate physical or digital security measures in place?** Relevant laws may require businesses to implement physical and digital security measures to protect the biometric data they collect and possess. Businesses designing data security measures to meet these requirements must take care to consider relevant industry standards, as well as controls the businesses may already be using to protect other sensitive data.

Perkins Coie's team of biometric law lawyers have deep experience advising clients on the use and development of biometric technologies and litigating cases relating to biometric data and biometric privacy. For further information, please send an inquiry to biometrics@perkinscoie.com or contact one of the authors directly.

Authors

Nicola Menaldo

Partner
NMenaldo@perkinscoie.com 206.359.8000

Ryan Spear

Partner
RSpear@perkinscoie.com 206.359.3039

Justin Potesta

Counsel
JPotesta@perkinscoie.com 737.256.6137

Explore more in

Privacy & Security Technology Transactions & Privacy Law Digital Media & Entertainment, Gaming & Sports Music, Film & Television

Related insights

Update

‘Tis the Season… for Cybercriminals: A Holiday Reminder for Retailers

Update

Employers and Immigration Under Trump: What You Need To Know