KPMG

Regulatory Alert

Regulatory Insights

May 2023

Biometric Information: Federal Trade Commission UDAP

KPMG Regulatory Insight:

- *The policy statement widely defines what may be considered "biometric information", such that all industries/companies should assess their collection and use of consumer biometric information.*
- *Expectations for compliance apply to companies and third parties (including affiliates, vendors, and end users) handling consumer biometric information (and data "derived from these sources of information") over the data "lifecycle", including collection, use, and extrapolation/estimation.*
- *The FTC intends to use existing UDAP regulation to cover emerging risks from the growing use of innovative technologies and "automated systems", which includes Artificial Intelligence and/or Generative AI technologies (see also KPMG Regulatory Alert, here).*
- *Companies should assess practices and controls against the examples provided but recognize this is a non-exhaustive list; FTC also notes that other laws and regulations may govern the collection, use, or storage of biometric information including the Children's Online Privacy Protection Act and the Safeguards Rule under the Gramm-Leach-Bliley Act.*

In response to the increasing use of consumer biometric information and related marketing of technologies that purport to use biometric information, the Federal Trade Commission (FTC) has adopted a policy statement on potential violations of the FTC's prohibitions on Unfair or Deceptive Acts or Practices (UDAP/Section 5 of the FTC Act) with regard to the collection and use of biometric information as well as claims regarding related technologies.

Policy Statement on Biometric Information

"Biometric Information". For purposes of the policy statement, "biometric information" refers to data that depict or describe physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person's body, including, but not limited to:

- Depictions, images, descriptions, or recordings of an individual's facial features, iris or retina, finger or handprints, voice, genetics, or characteristic movements or gestures (e.g., gait or typing pattern)
- Data derived from these sources of information

Emergent Risks. The FTC denotes examples of new and increasing risks associated with the collection and use of biometric information, including:

- *"Deepfakes"* or counterfeit videos or voice recordings that allow bad actors to convincingly impersonate individuals in order to commit fraud or to defame or harass the individuals depicted.
- *Large databases* of biometric information, which could be attractive targets for malicious actors seeking unauthorized access to devices, facilities, or data.
- *Location data*, which could reveal sensitive personal information about individuals with unintended

consequences (e.g., types of healthcare or attendance at religious, political, or union meetings).

— *Differential outcomes/treatment*, where technologies may perform differently across demographic groups (e.g., facial recognition or voice recording technologies).

UDAP/Section 5 of FTC Act. The policy statement includes a non-exhaustive list of examples of biometric information collection and use practices that may be considered "unfair" or "deceptive" under UDAP, including:

— False or unsubstantiated marketing claims relating to the validity, reliability, accuracy, performance, fairness, or efficacy of technologies using biometric information.

— Deceptive statements about the collection and use of biometric information.

— Failing to assess foreseeable harms to consumers before collecting biometric information.

— Failing to promptly address known or foreseeable risks, including failing to identify and implement readily available tools for reducing or eliminating risks.

— Engaging in surreptitious and unexpected collection or use of biometric information.

— Failing to evaluate the practices and capabilities of third parties, including affiliates, vendors, and end users that will be given access to consumers' biometric information or charged with operating biometric information technologies.

— Failing to provide appropriate training for employees and contractors.

— Failing to conduct ongoing monitoring of technologies that the business develops, offers for sale, or uses in connection with biometric information to ensure they are functioning as anticipated, are being operating as intended, and are not likely to cause harm to consumers.

For more information, please contact Amy Matsuo, Steve Stein, or Orson Lucas.

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com

kpmg.com/socialmedia