KPMG

Regulatory Alert

Regulatory Insights

January 2025

AI and Privacy: A Look at Biometric Tech & Data

KPMG Insights:

- ***Divergent Rulemaking:*** *States will continue to expand AI and privacy rulemaking (including and/or separate from biometric tech and data), resulting in increasing regulatory disparity.*
- ***Sensitive Data:*** *The definition of sensitive data will continue to expand, including but not limited to biometric data, geolocation data, etc.; this will be determined both through ongoing rulemaking and through litigation.*
- ***Regulatory Frameworks:*** *Companies should look to the array of regulatory frameworks, guidance and 'best practices' (as well as enforcements) to help gauge evolving risk management and governance expectations.*

In recent years, there has been a proliferation of biometric information technologies and applications, enabled in large part by AI and machine learning tools. The expanding collection and use of this information poses evolving and increasing risks to both consumers and businesses, spanning concerns such as data security, national security, privacy, fairness, and civil rights. Federal agencies and state authorities are taking actions to mitigate these risks under their jurisdictions, often within the context of AI- and privacy-related legislation, regulation, and/or enforcement. In the absence of an overarching federal law for AI or data privacy, multiple definitions and approaches for "biometric information" and related technologies are in place. An overview follows covering:

1. Trends in Biometrics Laws and Regulations
2. Frameworks, Guidance and Best Practices
3. Enforcement Activities

1. Trends in Biometrics Laws and Regulations

Recent actions by federal and state authorities to establish or enhance consumer protections related to the collection, use, disclosure, and/or monetization of biometric data include:

- **Federal Agencies:**
  - **FTC:** The Federal Trade Commission (FTC) issued a Policy on Biometric Information in response to concerns that the increasing use of biometric information and related technologies (e.g., AI, machine learning) raises "significant" consumer privacy and data protection concerns as well as the potential for bias and discrimination. The FTC identifies practices that it will scrutinize to determine whether companies collecting and using biometric information or marketing or using biometric information technologies are complying with the FTC's prohibitions on unfair or deceptive practices (see list below). For purposes of the Policy Statement, "biometric data" is defined to include depictions, images, descriptions, or recordings (and related derivative data) of an individual's faceprints, finger- and handprints, iris or retina scans, genetic data, and behavioral data that could identify an individual, such as walking gait and typing patterns.
  - **DOJ:** In December 2024, the Department of Justice (DOJ) issued a final rule that restricts transactions concerning "Americans' bulk sensitive personal data," including biometric identifiers, precise geolocation data, and personal health data with parties and individuals in countries of concern. The restrictions are intended to address "extraordinary" national security concerns, including malicious cyber-enabled

activities, targeted personal risks to U.S. persons (e.g., blackmail, coercion, intimidation), and misuse of data to develop and enhance AI capabilities and algorithms. The DOJ affirms a broad definition of biometric identifiers that includes facial images, voice prints and patterns, retina and iris scans, palm- and fingerprints, and behavioral data such as gait and keyboard usage patterns. Licenses must be obtained for otherwise prohibited or restricted transactions.

- **CFPB:** The Consumer Financial Protection Bureau (CFPB) released guidance (Circular 2024-06), which states that the use of biometric information in employment decisions must adhere to the Fair Credit Reporting Act (FCRA), including reports provided by third-party vendors to the employer. This includes data such as keystroke frequency, driving habits, and similar on-the-job monitoring to assess workers for productivity, risks to employers. or predictions on worker behavior (e.g., likelihood to leave job). Use of consumer reports that employ algorithms derived from biometric information must also conform to requirements of the FCRA (e.g., consent, transparency, disputes, limits). Per the FCRA, employers must obtain permission to use such reports for employment purposes and must provide notice to employees, along with a copy of the report, before taking adverse action.
- **FCC:** The Federal Communications Commission (FCC) adopted final rules that expand the scope of its data breach notification rules applicable to telecommunications carriers and interconnected VoIP providers as well as the definition of "covered data" to include biometric, genetic, or medical data.

— **State Authorities:**

Many states, including Illinois, California, Texas, Colorado, Washington, and Utah, have enacted privacy laws that govern the use of biometric data. This growing body of laws diverges in requirements and definitions of biometric data between individual states, in some cases broadening certain privacy protections beyond federal requirements. Examples of select state requirements include:

- **Illinois:** The Biometric Information Privacy Act (BIPA) requires a business or employer to receive informed consent before collecting biometric data. Illinois law holds third parties handling data to the same compliance standards. Private entities must develop a publicly available, written retention policy for biometric data.
- **California:** The California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) require businesses to inform consumers of biometric data collected and how long they will be retained. They give consumers the right to compel deletion. Differing from the Illinois law, the CCPA holds controllers of data, such as employers, to greater liability than third-party processors, requiring controllers to monitor the compliance of processors.
- **Texas:** The Capture or Use of Biometric Identifier Act (CUBI) prohibits capture of retina or iris scans, fingerprints, voiceprints or records of hand or face geometry without informed consent prior to capture. With some exceptions, the CUBI restricts the sale, lease, or disclosure of biometric identifier data and requires destruction of biometric identifiers within a year after the purpose for their collection expires.
- **Colorado:** In May 2024, Colorado amended its consumer privacy law to add protections for individuals biometric data including requiring informed consent when gathering biometric data, restricting employers' collection of biometric identifiers, and establishing written policies addressing disclosure and consent requirements, data retention and deletion, and security incident response. The law's definition of "biometric data" excludes facial or voice representation or data derived from either, unless used for identification purposes. An additional law expanded the definition of "sensitive data" to include biological data, which includes protections for "neural data".
- **Washington:** Washington's My Health My Data Act expands the definition of protected "consumer health data" beyond HIPAA to encompass "data that identifies the consumer's past, present, or future physical or mental health status," including biometric data (e.g., vein patterns, voice recordings) and other sensitive health-related data (e.g., precise location data). Any data generated from measurement or processing of physical or behavior characteristics may be protected and require informed consent to be collected or shared.

2. Frameworks, Guidance and Best Practices

The use of biometric technologies raises concerns about impacts on fairness, privacy, civil rights, and civil liberties. Risks related to the collection, use, disclosure, and/or monetization of consumer biometric data can impact both individuals and businesses and may include identity theft, fraud, misidentification/false positives, bias/discrimination, targeted malintent, and cyber security threats. Examples of guidance and best practices intended to mitigate these risks include:

- **FTC:** In its Policy on Biometric Information, the FTC stresses that businesses should implement "reasonable" privacy and data security measures to ensure that any biometric information they collect or maintain is protected from unauthorized access—whether that access stems from an external cybersecurity intrusion or an internal incursion by unauthorized employees, contractors, or service providers. In addition, businesses that use biometric information or biometric technologies should:
  - Assess foreseeable harms to consumers before collecting information.
  - Address known or foreseeable risks and identify and implement readily available tools to mitigate the risks.
  - Provide clear and conspicuous disclosure of the collection and use of biometric information and provide consumers with the right to opt-in or opt-out and a mechanism for complaints/disputes.
  - Evaluate the practices and capabilities of third parties, including affiliates, vendors, and end users, given access to consumers' biometric information or charged with operating biometric information technologies.
  - Train employees and contractors interacting with biometric information or related technologies.
  - Conduct ongoing monitoring of technologies the business develops, offers for sale, or uses in connection with biometric information to ensure that the technologies are functioning as anticipated and are not likely to harm consumers.

- **DOJ/DHS:** In December 2024, DOJ and the Department of Homeland Security (DHS), in collaboration with the White House Office of Science and Technology, jointly issued a report on biometric technology that details "best practices" for the agencies' use of biometric information and related AI tools, including:
  - Prohibiting the use of AI models trained on biometric data known to be captured in violation of existing laws, including state and local laws, or in violation of existing Federal government guidance.
  - Assessing the provenance of data used to train or fine-tune AI models and requiring vendors to provide information on provenance, if possible, to verify that the data conform to laws and regulations.
  - Documenting policies and procedures for the acceptable use of biometric technologies (e.g., facial recognition) and establishing policies and procedures to address improper use.
  - Establishing quality criteria for biometric data and the minimum accuracy of biometric technology systems, aligning with standard-setters such as NIST (National Institute of Standards and Technology under the Department of Commerce).
  - Assessing and benchmarking biometric systems using standardized methodologies in as close to an operational context as possible.
  - Requiring technical and policy training for personnel who use biometric technologies.
  - Retaining detailed internal logs of biometric system use and testing for auditing and compliance.

3. Enforcement Actions

Examples of recent enforcement actions across federal agencies and state authorities include:

- **FTC:** Significant monetary penalties and increase privacy restriction on companies concerning the use of biometric information (e.g., facial recognition technology) under its UDAP authority, including requirements associated with disclosure, informed consent, data deletion, and accountability. Additionally, settlements have required companies to delete models and algorithms developed using biometric data or have prohibited a company from using AI-based technologies for specific data collections altogether for a period of years.
- **State Authorities**: Lawsuits entered into by individual states regarding the collection and use of biometric information and technologies, largely based on misrepresentations of data collection

features, failure to provide notice of the data collection, or failure to obtain consumer consent, include a variety of contexts such as:

- Photos posted to social media.
- Surveillance cameras/technologies in retail settings.
- Surveillance activity in workplace settings.
- Misidentification (e.g., profiling, wrongful arrest).
- Sales of data to third parties (e.g., driving data to insurance companies).
- Failure to protect data from misuse/unauthorized access (e.g., data breach).

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

Contact the author:

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