CLIENT ALERTS & INSIGHTS

FTC Implements Broad Definition of Biometric Information; Increases Focus on Data Protection Impact Assessments

MAY 31, 2023

While States like Illinois, Texas, and Washington focused on opt-in consent; the FTC is focused on clear and conspicuous disclosures and accounting and planning for foreseeable harms related to the collection of biometric information.

On May 18, 2023, the Federal Trade Commission (the "FTC") released a new policy statement on biometric information, which set forth a clear indication that the FTC will focus its Section 5 FTC Act enforcement authority over those businesses collecting or using biometric information in deceptive or unfair manners.

Regulating biometric information collection and use is not uncommon in the United States, as Illinois, Texas, and Washington all have laws requiring prior opt-in consent before collecting an individual's biometric information. Major cities such as New York City and Baltimore have also passed local ordinances on biometric information collection and use.

In Illinois specifically, litigation has increased, with the first Biometric Information Protection Act ("BIPA") trial resulting in a $228 million judgement. In February, the Illinois Supreme Court also determined that BIPA claims accrue each time a business collects a single data point that falls under the biometric information category (e.g., each time some's fingerprint is scanned).

Even the new, broad omnibus U.S. state data protection laws that have proliferated in the absence of federal government action on the collection of personal information generally, have implemented the idea of "sensitive information," which includes biometric information. Depending on the state, the collection and use of sensitive personal information requires prior opt-in consent and/or providing an individual the ability to opt-out of the collection and use of their sensitive personal information.

Now though, the FTC appears poised to increase its investigatory and enforcement activity related to unfair and deceptive business practices by leveraging a broad definition of what it considers to be biometric information and what it considers to be "significant concerns with respect to consumer privacy, data security, and the potential for bias and discrimination."

Definition of Biometric Information

U.S. state laws, such as in Illinois, traditionally set forth a narrow scope of what they considered to be biometric information. Specifically, the U.S. state laws have focused on a sub-set of "biometric identifiers" such as retina or iris scans, finger or handprints, voiceprints, or scans of an individual's facial geometry. Additionally, the identifiers would need to be used in a manner that is intended to identify the specific individual.

The FTC, however, in its latest policy statement makes clear it is focused on a larger swath of identifiers and information related to biometric identifiers.

The FTC defines "biometric information" as "data that depict or describe physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person's body." The policy statement also includes a non-exhaustive list of what have becomes traditional biometric information examples: (i) facial geometry and features; (ii) iris or retinas; (iii) finger or handprints; (iv) voiceprints; or (v) genetics.

However, the policy statement also gives examples of what is considered "biometric information" that go far beyond what traditional biometric information laws previously identified, such as, an individual's characteristic movements or gestures (e.g., gait, typing patterns, etc.). Further broadening the definition of is that the FTC considers any data derived from depictions, images, descriptions, or recordings of an individual's biometric information to also be biometric information-meaning the output form analyzing an individual's biometric information would be considered biometric information.

Another example of how broadly the FTC's definition of biometric information reaches is that it would also include an individual's typing patterns. Tools analyzing typing patterns have become more and more common in the employer-employee relationship during the post COVID-19 pandemic work from home era as a tool for employers to measure productivity. Under the FTC's policy statement, such tools would be subject to biometric information considerations. This will increase the need for employers to consider what is and is not biometric information when crafting employee and job applicant privacy notices.

FTC Authority; Specific Biometric Information Considerations

Generally, under the Federal Trade Commission Act (the "FTC Act"), the FTC has broad investigatory and enforcement power aimed at protecting consumers from unfair and/or deceptive business practices.

Under the FTC Act, a practice is unfair if it (1) causes or is likely to cause substantial injury to consumers; (2) the harm is not reasonably avoidable by consumers; and (3) the harm is not outweighed by countervailing benefits to consumers or competition. Although violations of the law may be relevant, the existence or substantial likelihood of injury is the key determination, not the illegality of the act.

The deceptive prong of the FTC's investigatory and enforcement powers is more straight forward and typically involves a business publicly committing to one thing, but not following through on such commitment(s). For example, where a privacy notice promises to delete all data after a certain period of time, but where the data is actual kept far beyond that time period.

Regarding biometric information, the FTC policy statement sets for a "non-exhaustive" list of practices the FTC will scrutinize.

"Deception" in the biometric information space-according to the FTC includes "false or unsubstantiated marketing claims relating to the validity, reliability, accuracy, performance, fairness, or efficacy of technologies using biometric information." Deception can also include other

"deceptive" statements a business (whether they are the technology provider or user) makes about the collection or use of biometric information.

The last point is crucial, as the FTC will be looking to both the providers of biometric information technologies and the businesses that use such services.

"Unfairness" under the policy statement includes activity whereby a business:

- fails to assess foreseeable harms to consumers before collecting biometric information;
- fails to promptly address known or foreseeable risks;
- engages in surreptitious and unexpected collection or use of biometric information;
- fails to evaluate the practices and capabilities or third parties;
- fails to provide appropriate training for employees and contractors; or
- fails to conduct ongoing monitoring of technologies that the business develops, offers for sale, or uses in connection with biometric information.

Considerations for Businesses Moving Forward

Even before the FTC put out its latest policy statement-with class actions growing exponentially in states like Illinois-businesses needed to closely scrutinize their biometric information collection and use practices.

The FTC policy statement now puts forth examples of how businesses should be analyzing such practices. For example, businesses should incorporate discussions and reviews of any foreseeable harms that could come from the misuse of the in-scope biometric information and conduct on going due diligence of any current or new biometric information service providers.

Businesses that collect and use biometric information also need to ensure they have clear public-facing (e.g., to employees or consumers depending on those identified by the technologies) notices that are accurate to the biometric information practices and that clearly set forth how that information is used.

As the FTC and the Federal Government increase their focus on broad regulations related to the collection and use of consumer personal data, the Benesch Data Protection team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.