MINTZ

The FTC Sets Its Sights on Biometric Information

July 06, 2023 | Blog | By **Christopher J. Buontempo**, **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

- Privacy & Cybersecurity

RELATED INDUSTRIES

- Technology

Does your business collect or use fingerprints? Do your building access points use retina, finger, or palm scans? Does your security office use facial recognition technology to identify repeated trespassers? Do your phone systems use voice recognition technology? If you answered yes to any of these questions, your organization collects and uses biometric information. It is also important to think about your business' own products and services, and specifically, whether those products and services collect, use, or rely on biometric information.

These questions are not typically top of mind for legal and compliance teams, however, based on a recent Federal Trade Commission ("FTC") **policy statement**, they soon should be. The recent policy statement focuses on how use of emerging technologies that use biometric information might harm consumers and violate the FTC Act. The guidance is useful for both business that use biometric technologies in their own products and services, as well as for businesses that use biometric technologies provided by third party vendors.

In its statement, the FTC cites "*The increasing use of consumers' biometric information and related marketing of technologies that use or purport to use biometric information raise significant concerns with respect to consumer privacy, data security, and the potential for bias and discrimination.*" Similarly, Samuel Levine, Director of the FTC's Bureau of Consumer Protection, noted "*In recent years, biometric surveillance has grown more sophisticated and pervasive, posing new threats to privacy and civil rights.*"

Technological advancements in recent years has vastly increased the proliferation of biometric information technologies. If you have had your fingerprints taken, used voice or facial recognition technology, or used DNA ancestry testing, your biometric information was collected. However, your biometric information may also be collected and used in ways that are not always apparent. Many retail stores, airports, and other physical establishments use facial recognition technologies that collect and rely on use of biometric information. The FTC has taken note of all of this, and its recent policy statement may be a shot across the bow.

What is "biometric information?"

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.*" This includes, but is not limited to, the following: 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), as well as data derived from such depictions, images, descriptions, or recordings, to the extent that it would be reasonably possible to identify the person from whose information the data was derived. For example, both a photograph of a person's face and a facial recognition template, embedding, faceprint, or other data that encode measurements or characteristics of the face depicted in the photograph are considered "biometric information."

Current Legal Landscape

Biometric information has been regulated for several years under state law in Illinois, Texas, and Washington. Additionally, biometric information is regulated under general state privacy laws such as the California Consumer Privacy Act. However, there is no federal law that specifically regulates biometric information. The FTC, in its typical fashion as of late, signals that it is willing to fill that perceived gap by utilizing Section 5 of the FTC Act – which broadly prohibits unfair or deceptive acts or practices in or affecting commerce - as a means to regulate biometric information.

Notably, the fines for non-compliance with current state biometric information laws can be quite significant. For example, violation of Illinois' Biometric Information Protection Act (BIPA) carries fines up to $1,000 per violation for negligent violations, and $5,000 for intention or reckless violations. If that was not a deterrent enough, the Illinois Supreme Court in Cothron v. White Castle recently clarified that separate BIPA violations accrue ***each and every*** time an organization scans or transmits an individual's biometric information – which can easily result in astronomical penalties. For example, if a business

scans an employee's fingerprint each day in order to allow facility access, ***a separate claim accrues each and every time that the employee's fingerprint is scanned to enter the facility.*** Start doing the math…

And, a recent US Court of Appeals ruling in the Seventh Circuit marked the first time that an appellate court provided a roadmap to insurance carriers regarding policy language that the Court said was too vague to exclude coverage for a policyholder that allegedly violated BIPA. The **ruling** obligates an insurance carrier to pay an IT vendor's legal bills in two proposed BIPA class actions. The Court's ruling gives carriers a strong message about the type of specificity courts expect to see in policy language if the carriers want to exclude coverage for BIPA. If your company potentially has BIPA exposure, read your policy carefully (or contact **our Mintz experts** to assist).

How Biometric Technologies intersect with The FTC Act

The policy statement includes a non-exhaustive list of examples of practices that the FTC will scrutinize in determining whether companies that collect and use biometric information are comply with Section 5 of the FTC Act.

Deceptive Practices

The policy statement draws attention to "false or unsubstantiated marketing claims relating to the validity, reliability, accuracy, performance, fairness, or efficacy of technologies using biometric information." The FTC specifically warns against making claims without a reasonable basis, including claims that biometric technologies will deliver particular results or outcomes.

The FTC notes that false or misleading statements about the collection and use of biometric information constitute deceptive acts in violation of Section 5 of the FTC Act, as does failing to disclose any material information needed to make a representation non-misleading. Additionally, the policy statement guides businesses not to make false statements about the extent to which they collect or use biometric information or whether or how they implement technologies using biometric information.

Unfair Acts

The policy statement makes clear that the use of biometric information or biometric information technology may be an unfair practice within the meaning of the FTC Act.

The FTC draws upon its previous enforcement actions, noting that "collecting, retaining, or using consumers' personal information in ways that cause or are likely to cause substantial injury, or disseminating technology that enables others to do so without taking reasonable measures to prevent harm to consumers can be an unfair practice in violation of Section 5 of the FTC Act."

How to Avoid Liability under the FTC Act

Reasonable Privacy and Information Security

According to the policy statement, "in order to avoid liability under the FTC Act, businesses should implement reasonable privacy and data security measures to ensure that any biometric information that they collect or maintain is protected from unauthorized access."

Factors in the FTC's Assessment

The FTC notes that determining whether a business's use of biometric information or biometric information technology violates Section 5 "requires a holistic assessment of the business's relevant practices."

There are several factors that the FTC will use in its analysis (though the list is not exhaustive) of whether a business is violating Section 5 in connection with its use of biometric technologies:

- ***Failing to assess foreseeable harms to consumers before collecting biometric information*** - (Prior to collecting biometric information or using biometric information technology, businesses should conduct a holistic assessment of the potential risks to consumers)
- ***Failing to promptly address known or foreseeable risks*** – (this includes failing to identify and implement readily available tools for reducing or eliminating risks)
- ***Engaging in surreptitious and unexpected collection or use of biometric information.*** (In some situations, use of biometric technologies may be unfair in and of itself, such as, for example, using biometric technology to surreptitiously identify or track a consumer in a manner that exposes the consumer to risks such as stalking, exposure to stigma, reputational harm, or extreme emotional distress)
- ***Failing to evaluate the practices and capabilities of third parties*** - (this includes due diligence, assurances, contractual obligations, and ongoing oversight to ensure that third parties, including affiliates and vendors, that will have access to biometric information or will use biometric technologies are meeting appropriate requirements)

- ***Failing to provide appropriate training for employees and contractors*** – (this includes all personnel that interact with biometric information or related technologies)
- ***Failing to conduct ongoing monitoring of technologies that the business develops, offers for sale, or use in connection with biometric information*** (this is meant to ensure that the technologies are functioning as anticipated, that users of the technology are operating it as intended, and that use of the technology is not likely to harm consumers)

A Bridge Too Far

According to the FTC, in some situations, the adoption of a contemplated practice that uses biometric information may be unjustifiable when weighing the potential risks to consumers against the anticipated benefits of the practice. For example, if more accurate, less risky alternatives are available, using a technology that is proven to have high error rates may present an unjustifiable risk to consumers, even if the technology is more convenient, more efficient, or more profitable for the business considering implementing the technology.

Takeaways

Do you know whether your organization collects or uses biometric information, or more directly, does your company's products or services collect, use, or rely on biometric information? Now is a good time to find out. As organizations grow, it is quite common for technology to roll out across various departments that is not always flagged as carrying privacy or data protection risks, and this can easily include biometric information technology. Also, keep your third party vendors and service providers in mind when conducting this review, as they may be collecting or using biometric information as part of the products and services that they are providing to your organization – and your organization may be on the hook for it.

If you discover that your organization collects or uses biometric information, or if you need a bit of help finding out, contact the **Mintz Privacy and Cybersecurity Team** to shepherd you through this very thorny legal area.

Authors

Christopher J. Buontempo, Associate

Christopher J. Buontempo is a Mintz corporate attorney and a Certified Information Privacy Professional (CIPP). He has significant experience handling issues relating to technology, data privacy and security, brand protection, contract negotiation, licensing, and product development.

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.