PAUL HASTINGS

Stay Current

June 2023

Follow @Paul_Hastings

Biometrics in Focus at the FTC

By Adam Reich & Jeremy Berkowitz

Introduction

Two recent actions by the Federal Trade Commission ("FTC") reveal a potentially significant shift in its regulatory and potential prosecutorial focus to companies that use, obtain, share, disclose, disseminate, and/or store biometric information.

Possible COPPA Prosecutions Relating to Biometric Data

On June 5, 2023, the FTC disclosed a proposed order in connection with an action that it initiated against a public company manufacturer of video game consoles, which expressly includes "biometric data," such as "eye tracking, iris and retina scans, voiceprint, scan and hand and face geometry, fingerprint, and gait," among the "Personal Information" regulated by the Children's Online Privacy Protection Act ("COPPA"). (Proposed Order at Definitions, ¶ P.) In a related Press Release, the Director of the FTC's Bureau of Consumer Protection emphasized that the action and the Proposed Order "make it abundantly clear that kids' . . . biometric data . . . are not exempt from COPPA." As the FTC has brought multiple enforcement actions under COPPA in recent years, obtaining broad injunctive orders and millions of dollars' worth of penalties in the process, these actions by the FTC may portend a new front for these COPPA prosecutions, which should not be ignored by companies operating or interacting with children's biometric data.

Possible FTC Act Prosecutions Relating to BIPA

On May 18, 2023, the FTC published a Policy Statement on Biometric Information and Section 5 of the Federal Trade Commission Act ("Policy Statement"), which sets out a "non-exhaustive list of examples of practices the FTC will scrutinize in determining whether companies collecting and using biometric information or marketing or using biometric information technologies are complying with Section 5 of the FTC Act." Based on the Policy Statement, this list includes:

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

2. deceptive statements about the collection and use of biometric information, including statements which involve untruthful information or half-truths;

3. collecting and using biometric information without clearly and conspicuously disclosing that such collection and usage is occurring;

4. conditioning access to essential goods and services on providing biometric information;

5. automatically and surreptitiously collecting consumers' biometric information as they enter or move through a store; and

6. failing to use reasonable data security practices with respect to biometric information.

As used in the Policy Statement, biometric information means "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, and data derived from, an individual's facial features; iris or retina; finger or handprints; voice; genetics; and characteristic movements or gestures (e.g., gait or typing pattern). In addition, the FTC expresses the unique viewpoint in its Policy Statement that a photograph of a person's face may be biometric information. *Compare, e.g.*, Policy Statement, ¶ 2 ("By way of example . . . a photograph of a person's face . . . constitute[s] biometric information.") *with* Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS 4/10 ("Biometric identifiers do not include . . . photographs . . . .").

While the FTC's Policy Statement does not have any binding legal effect, the accompanying press release issued by the FTC on the same date characterizes the Policy Statement as a "warn[ing] that false [or] unsubstantiated claims about the accuracy or efficacy of biometric information technologies or about the collection and use of biometric information may violate the FTC Act." This admonishment should not be taken lightly. While this statement is non-binding, the FTC has been known to use past Policy Statements as a basis for future rulemakings.

What Consumer Companies Need to Be Doing If They Are Not Doing It Already

In light of the FTC's recent actions relating to biometric data, as well as the Policy Statement's explicit identification of factors that the FTC will consider in evaluating whether a business's use of biometric information or biometric technology is "unfair" in violation of the FTC Act, consumer companies should immediately review their technology offerings and customer bases to determine if they fall within the potential ambit of the FTC's signaled interpretation of COPPA and the FTC Act. Such companies should also set a regular schedule for conducting such introspective reviews going forward. If the current introspective review leads a consumer company to conclude that it engages with biometric information through any of its technology offerings, then the company should consider the following additional steps:

1. Engage privacy counsel to either (a) review and, if necessary, revise, existing privacy policies, or (b) draft clear and comprehensive privacy policies that meet the requirements of COPPA and the FTC Act, as applicable;

2. Engage privacy counsel to review and, as necessary, draft or revise existing notices and consent mechanisms pertaining to biometric information collection;

3. Engage privacy and advertising counsel to review existing and contemplated marketing materials relating to company-produced or company-employed technologies that use, receive, obtain, or store customer biometric information;

4. Evaluate any published statements about accuracy and bias relating to biometric technology with counsel, to ensure such claims have been thoroughly tested against appropriate representative samples;

5. Consult with experienced information security professionals and privacy counsel to determine whether the company needs to employ different or additional data security practices with respect to biometric information;

6. Assess the consumer company's operations to determine whether biometric information, as interpreted by the FTC, is being collected in any instance without appropriate notice;

7. Design a mitigation plan, along with experienced counsel, for all identified privacy and security risks relating to biometric information, and actively track all mitigation efforts and compliance;

8. Evaluate the practices and capabilities of third parties, including affiliates, vendors, and end users, who may be given access to consumers' biometric information or otherwise tasked with operating biometric information technologies, and require all such third parties to have security and technical measures in place; and

9. Work with privacy and employment counsel to design and regularly deliver training for employees and contractors concerning the handling of biometric information.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

Adam Reich
1.312.499.6041
adamreich@paulhastings.com

Washington, D.C.

Jeremy Berkowitz
1.202.551.1230
jeremyberkowitz@paulhastings.com