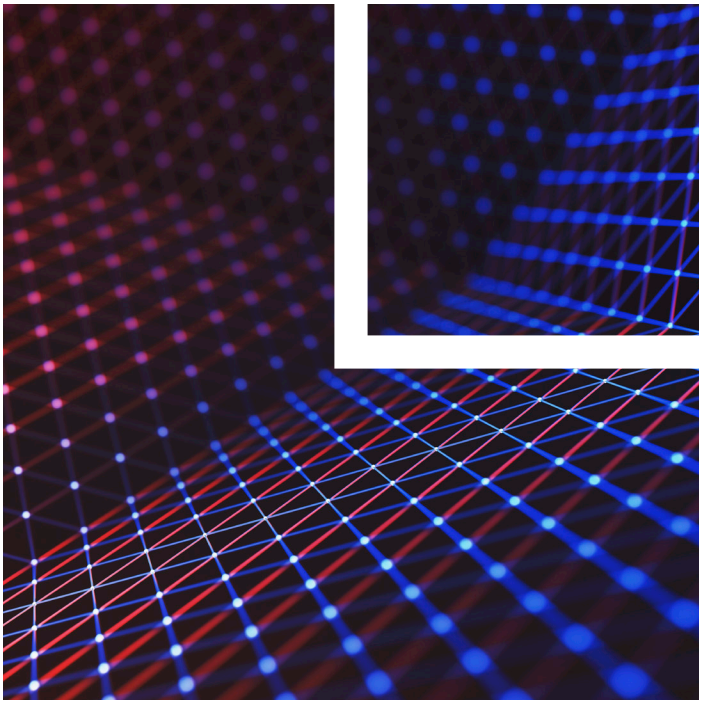
Advertising & Media Alert
March 2021

FTC, Federal and State Lawmakers Signal Focus on Biometric Data



The Federal Trade Commission (FTC) recently reached a proposed settlement with the California-based developer of a photo storage app accused of deceiving consumers about how it used facial recognition technology. Everalbum Inc., a technology company that develops and markets facial recognition technology for businesses, launched a consumer photo storage service and app with a feature that used facial recognition software to sort and tag users' photos. The company enabled the feature by default for most of its mobile app users and without the option to turn it off, in violation of its own stated policies.

That the FTC brought an enforcement action against Everalbum is hardly surprising—the agency has been pursuing technology companies that fail to live up to their own privacy representations for some time. But the proposed settlement with Everalbum over the use of facial recognition software goes far beyond any previous settlement in terms of the affirmative actions the app maker is required to take. This, together with a statement by Commissioner Rohit Chopra about the settlement, signals a shift in FTC enforcement policy around the use—or misuse—of facial recognition software and perhaps the larger category of biometric technology.

The FTC settlement is also one of the latest developments in the attempt to regulate at the intersection of individual privacy and emerging biometric technology, which identifies individuals using their faces, fingerprints, hands, retinas and irises, and voices, among other physiological markers, and includes facial recognition technology.

Key Takeaways:

- The Everalbum settlement required the deletion of tainted data. This signals a potential shift in how the FTC may enforce against future privacy violations (biometric or otherwise), since the requirement to delete the data collected is likely a more significant penalty than any fine.
- While no federal law exists at the moment regulating the collection and use of biometric data, the FTC has signaled that it intends to focus in this area.
- In recent years, federal lawmakers have proposed bills restricting or regulating the use of this technology, some of which indicate a bipartisan effort to exert federal control. With a new administration and control of both Congress and the executive branch in the hands of one party, additional pushes to enact federal privacy regulation—including covering biometric information and technology—are likely.
- A handful of states and several cities have enacted laws regulating the collection, use, storage and disposal of individuals' biometric data, with proposed new measures on deck for consideration in 2021.
- While only Illinois' biometric law includes a private right of action, the possibility that more states will enact legislation suggests that more litigation brought by consumers alleging the violation of their rights is on the horizon.

Everalbum Settlement Requires Deletion of Tainted Data

Everalbum's Ever app enabled users to upload photos and videos from their mobile devices, computers and social media accounts to the company's cloud-based storage

Attorney Advertising

service. According to the FTC, Everalbum launched a new feature in 2017 called "Friends" that used facial recognition technology to sort and tag users' photos and, between July 2018 and April 2019, represented to customers it would not apply the facial recognition technology to users' content unless users affirmatively chose to activate the feature. Instead, the company allowed Ever app users in only three states—Illinois, Texas and Washington—to decide whether to turn on the facial recognition feature, while activating the feature by default for all other users without the option to turn it off. As Commissioner Chopra pointed out in his statement on the settlement, Everalbum took greater care when it came to consumers in those three states because those are the only states that have laws regulating the collection and use of an individual's biometric information.

The FTC's complaint also alleges that Everalbum did not confine its misuse of facial recognition technology to Ever's Friends feature. Between 2017 and 2019, Everalbum collected millions of facial images through Ever and used those images, along with publicly available datasets, to compile four databases for use in its work to "train" artificial intelligence-driven facial recognition technology and services for its commercial clients, including those in the security and air travel industries. Everalbum also promised Ever users that it would delete the photos and videos of users who deactivated their accounts, but allegedly failed to do so until October 2019.

While the proposed settlement, announced Jan. 11, does not include any monetary penalties, it does require the company to delete all photos and videos of Ever app users who deactivated their accounts and all "face embeddings"—facial features data that can be used for facial recognition purposes—derived from the photos of Ever users who did not expressly consent. The settlement also requires that Everalbum delete any facial recognition models or algorithms developed through the use of Ever users' photos or videos—the first time the FTC has required this kind of action.

In his statement, Commissioner Chopra pointed out that the requirement under the settlement that Everalbum delete not just the consumer data but everything derived from it was a significant departure—what he called "an important course correction"—from previous settlements, referencing earlier actions in which larger tech companies were allowed to retain algorithms and other technologies developed or enhanced by what Chopra called "illegally obtained data."

The complete deletion requirement, which was approved unanimously by the five commissioners, as well as Commissioner Chopra's statement suggest that the FTC will be taking a harsher stance on penalties for companies that mislead consumers on the collection and use of biometric data, with potentially significant and costly consequences for companies developing and training facial recognition and other biometric technology and software.

Under the settlement, Everalbum is also prohibited from misrepresenting how it collects, uses, discloses, maintains or deletes personal information, including the data created through the use of facial recognition technology, and must accurately disclose the extent to which it protects the privacy and security of any personal information it collects. The company also has agreed to obtain the express consent of its users before applying facial recognition technology to their photos and videos.

According to a recent statement, the company discontinued its photo storage services and mothballed the Ever app in August 2020, and released its latest-generation Paravision face recognition model—which it represents does not use any of the data derived from Ever users—the following month.

State and Federal Efforts

Several states have enacted laws regulating the collection and use of individuals' biometric data, but no federal legislation is on the books yet.

Currently, only Illinois, Texas and Washington have specific laws regulating the use of biometric data. The first to be enacted, Illinois' Biometric Information Privacy Act (BIPA), which was passed in 2008, provides a private right of action. The California Consumer Privacy Act, which took effect on Jan. 1, 2020, covers a broad range of personal information, including biometric data. The California Privacy Rights Act (CPRA), passed by voters in November 2020 and effective Jan. 1, 2023, creates the new category of "sensitive personal information" that includes biometric data. The CPRA gives California residents the right to restrict the ability to use and sell that information. Virginia also recently passed the Virginia Consumer Data Protection Act, which, much like the CPRA, treats biometric data as part of the category of sensitive personal data.

Under both the California and Virginia laws, this category includes the processing of biometric data for the purpose of uniquely identifying an individual or consumer. Under

the CPRA, biometric data is defined to include, among other human characteristics, imagery of the face "from which an identifier template, such as a faceprint … can be extracted[.]" Virginia's new law, which is on the governor's desk for his signature, does not specifically mention faces or facial features, but defines biometric data as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual," which presumably would include facial features. The text of the law does exclude a "physical or digital photograph … or data generated therefrom."

Additional states, including Arkansas, Maryland and Oregon, have amended their existing privacy protection laws to expand the definition of personal information to include biometric information. Numerous other states have introduced biometric regulation bills in recent years, though none have passed so far. But a few states kicked off 2021 with new efforts.

In New York, Assembly Bill 27, introduced on Jan. 6, would require private entities in possession of biometric information to develop a written retention policy and guidelines for permanently destroying the biometric data. Under the bill, biometric data must be destroyed when the initial purpose for collecting the data has been satisfied or within three years of the individual's last interaction with the private entity, whichever occurs first.

Lawmakers in Utah recently introduced S.B. 34, which would regulate governmental use of facial recognition technology. S.B. 34 would limit the circumstances in which government entities may use image databases for facial recognition comparisons and outline the process of, and requirements for, conducting facial recognition comparisons. The bill also would require the government to notify Utah residents that their images and biometric information are used.

The city of Portland enacted a ban on facial recognition technology, which took effect on Jan. 1, and is the first city to prohibit private entities from using this technology. Private entities are broadly defined as businesses, associations or other legal entities doing business within the city limits. The ban applies to brick-and-mortar locations within the city limits, not to websites or other digital platforms.

At the federal level, there have been two recent attempts to pass federal biometric legislation. Most recently, U.S. Sens. Jeff Merkley, D-Ore., and Bernie Sanders, I-Vt., introduced the National Biometric Information Privacy Act of 2020 to regulate the collection, retention, disclosure and destruction of biometric information at the federal level. The bill included faceprints in the definition of biometric data and specifically mentioned those derived from photographs. The bill also required that private entities develop and make available to the public a written data retention policy, and had provisions addressing consumer notice and consent. In addition, among other limitations, the bill prohibited the disclosure, sale or use for advertising purposes of biometric information without express written permission of the subject. The bill authorized both a private right of action and actions by state attorneys general for violations, and provided for per-violation statutory damages. The bill died in Congress after failing to move past the committee stage.

Prior to that, Sens. Brian Schatz, D-Hawaii, and Roy Blunt, R-Mo., introduced the "Commercial Facial Recognition Privacy Act of 2019," a narrower, bipartisan bill focused on the use of facial recognition software. The bill prohibited the commercial use of facial recognition technology to identify and track consumers without consent. It also limited the sharing of collected faceprint data with third parties and imposed minimum data security standards. The bill exempted "security applications" for loss prevention or to detect criminal activity, as well as products or services designed for "personal file management or photo or video sorting or storage if the facial recognition technology is not used for unique personal identification of a specific individual"—an exemption that could apply to social media photo tagging services or photo-sharing apps. While there is no private right of action, S.847 provided that a statutory violation of covered statutory provisions shall be deemed an unfair or deceptive practice under the FTC Act and that state attorneys general would also have certain enforcement powers. That bill also languished and eventually died in the committee.

To date, there have been no bills introduced in the 117th Congress covering the use of biometric or facial recognition technology or the data collected and used by this technology.

Individuals' Lawsuits

Meanwhile, Illinois remains the only state where private individuals can file suit alleging their biometric information was collected and used without permission. Not surprisingly, hundreds of BIPA lawsuits are pending in Illinois. Most of these lawsuits are brought by employees against their employers, alleging the companies' collection and storage of biometric data, such as fingerprints or facial recognition scans, for security or timekeeping purposes violates BIPA mandates.

Shoppers also are filing suit. Isela Carmean filed a proposed class action against Macy's in August 2020, alleging it used facial recognition software developed by Clearview AI to identify shoppers on store security cameras. Macy's has moved to dismiss the suit, arguing that Carmean can't prove the store security cameras actually captured her biometric information.

Ongoing Review

With a new administration and the introduction of proposed legislation at the state and city levels, 2021 could see renewed progress on the regulation of biometric information collection and use. It's highly likely that a proposed federal law will be reintroduced this year and that additional states and cities across the country will follow the example of those states that already regulate the use of this personal information. At the same time, continually evolving technology will require the ongoing review and potential amendment of existing biometric regulations.

Related Professional

Nerissa Coyle McGinn . . . . . nmcginn@loeb.com

6594 REV1 03-05-2021