A PRACTICAL GUIDE TO BIOMETRIC INFORMATION LAWS

by CHRISTIANA E. STATE, AGUSTIN D. OROZCO, JACOB S. CANTER, AND SARAH RIPPY

From door locks to vending machines, proctoring exams, and time-keeping devices, biometrics technology is now prevalent in our everyday activities. The legal landscape surrounding the collection and use of biometric information is complex and developing rapidly. Due to increased litigation involving biometric information, regulatory scrutiny of biometrics technologies, and business disruption caused by such litigation and investigations, it is important for companies involved in the collection or use of biometric information to institute a compliant biometric information framework. The following FAQs are intended to provide a high-level overview of the current state of biometric data laws, their enforcement, and the legal risks associated with noncompliance.

1. What is biometric information?

Biometric identifiers are, generally, any metrics related to human behavioral, biological, or physical characteristics, such as: retina or iris scans, fingerprints, voiceprints, hand scans, or face geometry. The definition of biometric information, however, varies depending on the applicable law. The first state biometric law passed in the United States defines biometric information as information that is based on biometric identifiers and is used to identify an individual. *See* Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14 (2008) (BIPA).

Biometric information is treated as sensitive data by various comprehensive privacy laws that were recently passed in the United States (California, Colorado, Utah, Connecticut, and Virginia), and these laws impose various additional obligations for the collection, use, and sharing of biometric information. For example, state privacy laws have included the following under the definition of biometric

information: voice recordings, gait patterns, DNA, vein prints, data used to infer emotions, keystroke patterns or rhythms, sleep patterns, and health or exercise data that contain identifying information.

2. Is a photograph considered biometric information?

Although a photograph by itself may allow for the identification of a person using certain technical data extracted from the photo, BIPA explicitly states that biometric information does not include photographs. However, the data derived from a photograph, such as a scan of the face geometry or a faceprint that is derived from a photograph, have been considered by some courts to be biometric information. In doing so, courts have distinguished normal photographic images from facial geometric scans. *See e.g.*, *Sosa v. Onfido, Inc.*, No. 20-CV-4247, 2022 U.S. Dist. (N.D. Ill. Apr. 25, 2022).

3. Which laws currently regulate the collection and use of biometric information?

There is no generally applicable federal law that regulates the collection or usage of biometric information. The laws that govern the collection and use of biometric information can be separated into three categories: (1) comprehensive privacy laws that regulate the processing of all personal information, including biometric information; (2) dedicated biometric privacy laws that only address biometric information; and (3) local government laws limiting the use of biometrics.

States and foreign governments have passed laws regulating all personal information. Domestically, Colorado, California, Virginia, Connecticut, and Utah have each passed comprehensive privacy laws. From an international perspective, the European Union, the United Kingdom, Brazil, and China have each also enacted comprehensive privacy laws addressing biometric information.

There are far fewer jurisdictions with dedicated biometric laws. Texas, Illinois, and Washington are currently the only states with dedicated biometric privacy laws. While each of these biometric privacy laws contain fairly similar provisions, Illinois' BIPA is unique in that it provides a private right of action, whereas Texas and Washington each relies on its respective state Attorney General for enforcement.

Lastly, several municipalities have limited the use of certain biometric technologies by government and law enforcement or have imposed restrictions on the use of biometrics in the employment context. Certain states also have breach notification laws that include biometric information as part of the definition of "personal information."

4. How has the BIPA private right of action been used?

Through 2017, there had been approximately 300,000 BIPA claims filed across the United States with losses totaling approximately $1.4 billion. Since 2017, however, the number of BIPA claims filed more than doubled. Additionally, the total losses have swelled to approximately $6.9 billion, an increase of more than 400%. The volume of BIPA cases and losses has grown in tandem with technological advances. When BIPA was first passed in 2008, companies generally could not purchase facial geometry technology and engage in large collections of biometric data the way they do today. BIPA, which addressed a narrower scope of commercial activity when it first passed, is much more relevant to commercial activity and widely used technology today.

5. What is the risk for failing to comply with BIPA?

The legal risks for failing to comply with BIPA or other biometric laws can be substantial, including high damages awards, penalties, and injunctive relief, all of which can be very disruptive to a business. For example, entities found liable for negligently violating BIPA owe the greater of actual damages or $1,000 per violation, and entities found liable for intentionally or recklessly violating the law owe the greater of actual damages or $5,000 per violation. When a party alleges that a company has violated the law multiple times for hundreds of customers or employees, the potential damages can skyrocket. To this end, courts have approved BIPA settlements for hundreds of millions of dollars. Attorneys' fees and costs may also be awarded to the successful party that brings a BIPA case. Beyond legal liability, companies involved in BIPA litigation are often compelled to pay their own significant legal fees for discovery into sensitive and proprietary technical business information. Public BIPA litigation also exposes companies to copycat claims or regulatory investigations, which carry increase financial and legal risks.

6. What will regulators want to know if your company is subject to a cyber incident involving biometric information?

The number of cyber incidents and the losses associated with those incidents continue to increase every year. Regulatory scrutiny into how a company handles a cyber incident is heightened if biometric information is involved, due to its sensitive nature. Because biometric information can be used to track individuals' locations and actions, and that biometric information cannot be changed if compromised or stolen, individuals face a heightened risk for identity theft and unauthorized tracking in the event of a cyber incident involving biometric information. As a result, regulator inquiries after a cyber incident will largely be focused on preventing future crimes from happening and the company's remediation efforts.

Regulators, therefore, will closely investigate the who, what, when, and where of the incident. Investigating the type of incident that took place (ransomware, business email compromise, phishing, etc.) and where the incident took place (laptop, server, cloud, etc.) will only be a starting point for regulators. The government will focus on the number of individuals affected and the risks to the individuals in relation to the type of biometric information compromised, whether the incident has been contained, and the company's efforts to prevent incidents from happening in the future, including protecting individuals who have been affected by the incident.

7. How do you conduct an effective internal investigation in the event of an incident involving biometric information?

A critical step in answering any regulator's questions is conducting a thorough internal investigation. Incidents involving biometric information can lead to more complex investigations given the higher risks to individuals. Typically, the investigation should contain three key components: (1) a forensic investigation; (2) a legal review of internal policies and procedures; and (3) a review of management's role and responsibilities. The forensic investigation is necessary to collect evidence and understand how and where the incident took place. With respect to the second and third components of an investigation, regulators, specifically the U.S. Department of Justice, have been focused on corporate compliance, which implicates additional compliance efforts when biometric information is involved. A big part of that is whether the company had the appropriate biometric policies and procedures in place, whether it was updating its policies and procedures, particularly in

light of the rapidly changing legal landscape, and whether it was ensuring that the policies and procedures were being followed. Given the heightened obligations with regard to privacy compliance involving biometric information (see more information below), regulators will pay closer attention to how the company is complying with the applicable privacy and data security laws. Regulators will also want to know management's role with respect to the implementation of the compliance programs and the response to the incident.

The three components of the investigation should be run in parallel and the decision making needs to be centralized to avoid inconsistent or inaccurate information being provided to regulators. A thorough investigation helps demonstrate that the company was prepared, did not play a role in the breach, and took affirmative steps to prevent future incidents.

8. How active have regulators been in investigating compliance with biometric information laws?

Aside from BIPA and its private right of action, every other relevant law relies on regulators to enforce their biometrics provisions. In most states, the state Attorney General is responsible for enforcement. In California, however, the California Privacy Protection Agency will relieve the California Attorney General of its enforcement authority in July 1, 2023. Unfortunately, very little is known about how comprehensive state privacy laws will be enforced as only California's law is currently in effect and the California Attorney General's office has only pursued one enforcement action to date.

With respect to dedicated biometric privacy laws, regulators have been comparatively less active than private litigants in bringing claims. To be sure, the full extent of regulatory action is unknown because investigations can be confidential and can be resolved without any public notice, even if a financial settlement is reached. This is in part a function of the financial resources of a state attorney general's office. But it's also the case that regulators can make a large impact on commercial activity even when they bring actions more sparingly. For example, in February of 2022, the Texas Attorney General sued Meta Platforms, Inc. (Meta) because the Instagram platform's facial filtering technology allegedly violated the Texas biometric information law by allegedly failing to properly obtain the informed consent of Texans and disclosing biometric information to third-party applications for commercial benefits, among other allegations. In response, Meta disabled the augmented reality facial filters for Texas and Illinois residents in May of 2022, causing a notable public response. About a week later, Meta reinstated the facial filters, but included opt-in language that needed to be accepted to use the features.

9. What are the legal and financial risks if a regulatory investigation does not go well?

Biometric information laws across the states do not carry uniform legal and financial risks for companies. For example, companies that violate the Texas biometric information law are subject to penalties of no more than $25,000 per violation; those who violate Washington's biometric information law are subject to penalties of no more than $7,500 per violation; and those who violate California's biometric information law are subject to penalties of no more than $2,500 per negligent violation and $7,500 per intentional violation. But the negative consequences for failing to take an investigation seriously are equally serious in every state—not only will it ensure closer scrutiny from the investigating regulatory body, it will also risk additional scrutiny from other regulators within the same state and other states as well.

10. Is it likely that new laws regulating biometric information will be passed?

Yes. Of the eight existing state laws addressing the use and collection of biometric information, four were passed in the last two years. In addition to those laws that passed, over forty comprehensive privacy bills in twenty-nine states were introduced during the 2022 legislative session. The majority of these bills directly regulate the use and collection of biometric information. This number is up from twenty-six bills in twenty-four states introduced during the 2021 legislative session. In addition to these comprehensive bills, legislators also introduced dedicated biometrics bills in seven states. Federal legislators have also been active in this space. In the past two years, there have been two comprehensive privacy bills addressing biometrics that have garnered significant momentum. Though most of these bills do not make it beyond legislative committee, their existence reflects increased legislative interest with respect to biometric information. While the bills may not succeed initially, we expect legislators to return with next year's iteration in January.

11. What are the industry best practices for processing biometric information?

BIPA provides a helpful framework for establishing best practices, as it applies one of the most rigorous standards for protecting biometrics. Companies should: (i) publish and implement a written biometric retention policy; (ii) inform data subjects in writing of the specific purpose for collection, as well as the actual use and storage practices; and (iii) obtain a written release from data subjects consenting to the disclosed collection, use, and storage practices. Companies should also adhere to BIPA's prohibitions on selling biometric information.

In obtaining consent, the company should ensure that the individual acknowledges having read the company's privacy policy, as well as the more specific written notice regarding the company's collection and use of biometric information. Additionally, individuals should acknowledge consent to those policies and notices, as well as to the collection and use of individual biometrics, including the company's ability to share their biometric information with any service providers or third-party vendors.

Beyond instituting this framework, we also suggest reviewing any existing agreements with vendors and other third parties that may be involved in collecting or processing biometric information in order to ensure compliance with applicable law.

Agustin D. Orozco *is a partner at Crowell, focusing on White Collar & Regulatory Enforcement. He can be reached at aorozco@crowell.com.* ***Christiana E. State*** *is a senior counsel, practicing in Crowell's Corporate & Transactional and Privacy & Cybersecurity groups. Her email address is cstate@crowell.com.* ***Jacob S. Canter*** *is a Crowell associate doing Litigation & Trial work, and can be reached at jcanter@crowell.com.* ***Sarah Rippy*** *is also an associate, practicing in the Privacy & Cybersecurity group, and her email address is srippy@crowell.com.*

This article first appeared in Orange County Lawyer*, January 2023 (Vol. 65 No. 1), p. 30. The views expressed herein are those of the author. They do not necessarily represent the views of* Orange County Lawyer *magazine, the Orange County Bar Association, the Orange County Bar Association Charitable Fund, or their staffs, contributors, or advertisers. All legal and other issues must be independently researched.*