Checklist

Biometric Privacy Compliance

David J. Oberly, Blank Rome

Bloomberg Law

Biometric Privacy Compliance

Editor's Note: For an overview of biometric privacy developments, see this related piece.

Contributed by David J. Oberly, Blank Rome

Companies that collect and use biometric data in their business should routinely assess their data practices not only to satisfy current legal obligations but also to ensure compliance as new laws and regulations are adopted.

Define Biometrics

☐ Assess whether data collected is indeed biometric data.

☐ *Biometrics* entails measurable human physiological characteristics and behavioral activities that are used to identify and verify/authenticate individuals' identities, and the automated methods of recognizing or analyzing a person based on those characteristics.

☐ *Biometric data* generally encompasses data derived from automatic measurements of a person's physiological characteristics and behavioral activities.

Comment: Biometric privacy laws generally refer to "*biometric identifiers*" and "*biometric information*."

• *Biometric identifier* refers to specific measurements of an individual's physiological characteristics, such as a scan of face or hand geometry, fingerprint, retina or iris scan, or voiceprint. Biometric identifiers do *not* include things such as writing samples, photographs, human biological samples used for testing or screening, or physical descriptions such as height or weight.

• *Biometric information* refers to any information that is based on an individual's biometric identifier and used to identify an individual, but does not include information derived from items excluded under the definition of biometric identifier.

Examples: The most common example of a biometric identifier is a fingerprint used by an employer for time and attendance purposes. While temperature screening activities ordinarily do not involve the collection of biometric data, some advanced temperature screening technologies–such as thermal scanners with facial recognition capabilities–may involve the collection of biometric data.

☐ Document biometric data flows and inventory.

☐ Determine what biometric data is collected and used.

☐ Determine where biometric data is stored and maintained, including any third-party systems that store biometric data and, from a geographical perspective, where the servers are located.

☐ Map where biometric data flows from the time of collection through the organization and externally to vendors and service providers.

☐ Determine the length of time biometric data is retained and in what format(s).

Comment: To properly ascertain an entity's applicable biometric privacy legal obligations and security risks, it is important to understand what biometric data is possessed and how it is managed. To do this, a data mapping and inventory exercise should be completed. Generally speaking, this entails mapping and inventorying every piece of biometric data collected, used, stored, disclosed, and/or sold, as well as all biometric data processing activities.

Completing this exercise will allow for the development of a comprehensive understanding of where the collection of biometric data takes place, as well as what parts of the organization it passes through and where it is thereafter used and stored.

This data flow map and storage inventory can aid in complying with the rapidly growing maze of biometric privacy laws, and in particular:

- Proactively managing and safeguarding biometric data.
- Building out the necessary privacy and notice disclosures.
- Knowing when and how to obtain and record consent.
- Satisfying applicable data destruction requirements.

Biometric Privacy Policy

☐ Develop a publicly-available biometric privacy policy.

Comment: The biometric privacy policy should be distinguished from the company's general privacy policy. Companies may choose to revise their current policies or, alternatively, use a separate, independent biometric privacy policy that directly addresses the company's biometrics practices. As a matter of best practice, companies should consider a separate biometric privacy policy, when feasible, because it is easier for data subjects to identify biometric-specific collection practices when separated out from other privacy policy provisions.

- Include, at a minimum, the following:
  - Clear notice that biometric data is being collected, used, stored, and/or shared.
  - The type(s) of biometric data that are being collected, used, stored, and/or shared.
  - The current and reasonably foreseeable purposes for which the company uses or may use biometric data.
  - How biometric data will be used.
  - A description of the data security measures used to safeguard biometric data from unauthorized access, disclosure, or acquisition.
  - A description of the company's biometric data retention and destruction schedule.

Comment: The specific retention and destruction schedules and limitations vary between major biometric privacy statutes. For example:

- The Illinois Biometric Information Privacy Act (BIPA) requires biometric data to be destroyed when: (1) the initial purpose for collecting the data is satisfied; or (2) within three years of an individual's last interaction with the company, whichever occurs first.
- Texas' Capture or Use of Biometric Identifier Act (CUBI) requires biometric data to be permanently destroyed within one year after the date the purpose for collecting the data expires. Moreover, CUBI provides that biometric data collected for security purposes by an employer is presumed to expire at the end of the employment relationship.
- Washington's RCA 19.375 biometric privacy statute (also referred to as "Washington HB 1493") requires biometric data to be permanently destroyed when it is no longer needed to: (1) comply with a court order, statute, or public records retention schedule; (2) protect against or prevent actual or potential fraud, criminal activity, claims, security threats, or liability; or (3) provide the services for which the data was originally collected.

As a matter of best practice, companies should use a schedule that provides for biometric data to be destroyed as soon as practicable after the initial purpose for collecting the biometric data has been satisfied or, in the context of employers, when the employment relationship with a worker has ceased, as destroying biometric data at the earliest feasible juncture can significantly limit potential liability exposure—especially in the data breach context.

☐ Guidelines for permanently destroying biometric data.

Comment: Generally, an entity's biometrics vendor will have information regarding its method(s) for permanently destroying biometric data that can be used to describe the applicable data destruction guidelines in the biometric privacy policy.

☐ Determine and implement mechanisms to ensure the public availability of the biometric privacy policy.

Comment: At a minimum, this should entail inclusion on the company's public-facing website. For employers, the policy should also be disseminated to employees through email or any other electronic communication commonly used by the employer. Biometric privacy policies can also be posted (1) at the location(s) where biometric data will be collected by the company; (2) at all workplace entrance points; and (3) on all websites or other locations where organizational policies are maintained, including employee handbooks.

☐ Ensure that the biometrics policy is made available before the collection, capture, or use of biometric data.

Written Notice

☐ Display a written notice to all individuals before any biometric data is collected, captured, received, or otherwise obtained from those individuals.

Comment: Due to the rapidly-changing biometric privacy legal landscape and the anticipated influx of additional biometric laws, as a matter of best practice notice should be provided to (and consent obtained from) all individuals whose biometric data is being collected, which can significantly mitigate potential liability exposure.

☐ Written notice should conspicuously include, at a minimum, the following information:

- ☐ That biometric data is being collected, used, and/or stored by the company.
- ☐ The type(s) of biometric data that are being collected, used, stored, and/or shared.
- ☐ The current and reasonably foreseeable purposes for which the company utilizes or may utilize biometric data.
- ☐ How biometric data will be used.
- ☐ The length of time for which the company collects, uses, and stores biometric data.
- ☐ Guidelines and schedule for permanently destroying biometric data.
- ☐ A brief summary of the protective measures used to safeguard biometric data.

☐ Determine and implement mechanisms to ensure the notice is provided to all individuals before the time biometric data is collected.

Comment: Consider using more than one mechanism to provide the requisite notice. At a minimum, post the written notice at all points where biometric data is collected. For employers, the notice should be disseminated to employees through email or any other electronic communication method ordinarily used by the employer. Where feasible, also provide a copy of the notice directly to the individual immediately before his or her biometric data is collected.

Written Release/Consent

☐ Develop a standardized written release/consent form to be executed by all individuals providing their unequivocal consent for the collection, use, and sharing of their biometric data.

Comment: The release should specify current and reasonably foreseeable purposes for which the company utilizes or may utilize biometric data. If the scope of purposes included in the original release does not encompass later intended uses, additional consent should be obtained before using the biometric data for a materially different purpose.

A release that is executed electronically satisfies the requirement that the release be in "writing." For Illinois' BIPA, the release can be executed by the individual or his or her "legally authorized representative."

☐ Ensure that the written release provides the company with the ability to:

- ☐ collect and use the individual's biometric data; and

☐ disclose or disseminate the individual's biometric data to third parties for business purposes. While specific third parties do not have to be identified in the release, all current or anticipated business purposes should be specified in as much detail as possible.

Comment: It is important to remember that consent is required for two distinct activities: first, the initial collection of biometric data; and second, sharing or disclosing biometric data to any third party.

Further, under Texas' CUBI, biometric data must *not* be disclosed unless one of four narrow exceptions applies: (1) the individual consents to disclosure for identification purposes in the event of his or her disappearance or death; (2) the disclosure completes a financial transaction; (3) the disclosure is required or permitted by federal/state statute; or (4) the disclosure is made in response to a warrant.

Conversely, under Washington's RCA 19.375, consent is *not* required to disclose an individual's biometric data to a third party where one of five exceptions applies: (1) the disclosure is consistent with the initial notice and consent; (2) the disclosure is necessary to complete a financial transaction; (3) the disclosure is required by federal or state statute or court order; (4) the disclosure is completed with a third party that contractually promises no further disclosure and that the data will not be used in a manner that is inconsistent with the initial notice and consent; or (5) the disclosure is completed to prepare for litigation or participate in the judicial process.

☐ Ensure that the text of the release provides that, in its execution, the individual acknowledges that he or she has read the company's biometric privacy policy, as well as the more specific written notice regarding the collection and use of biometric data, and that the individual consents to these policies and guidelines.

☐ Develop procedures and protocols to follow when individuals refuse consent. In such situations, the entity must ensure that it does *not* collect or use the individual's biometric data under any circumstances.

☐ Develop a process for maintaining detailed records of how and when consent is obtained.

Comment: While there is no requirement that individuals be verified before executing their written release, as a matter of best practice, it is best to verify the identity of individuals whenever feasible, and to document this verification process as well.

Limitations on Selling, Leasing, or Otherwise Profiting from Biometric Data

☐ Adhere to any requirements or limitations in connection with selling, leasing, or otherwise profiting from biometric data.

Comment: Illinois' BIPA places a strict prohibition that bars selling, leasing, trading, or otherwise profiting from individuals' biometric data.

Texas' CUBI provides that biometric data must not be sold or leased unless one of four narrow exceptions applies: (1) the individual consents to disclosure for identification purposes in the event of his or her disappearance or death; (2) the disclosure completes a financial transaction; (3) the disclosure is required or permitted by federal/state statute; or (4) the disclosure is made in response to a warrant.

Washington's RCA 19.375 provides that consent must be obtained before selling or leasing an individual's biometric data, subject to five exceptions where consent is not required: (1) the activity is consistent with the initial notice and consent; (2) the activity is necessary to complete a financial transaction; (3) the activity is required by federal or state statute or court order; (4) the activity is completed with a third party that contractually promises no further disclosure and that the data will not be used in a manner that is inconsistent with the initial notice and consent; or (5) the activity is completed to prepare for litigation or participate in the judicial process.

☐ Implement mechanisms to ensure that all requirements and restrictions on selling, leasing, or otherwise profiting from biometric data are satisfied.

Comment: Companies may consider developing a checklist for personnel to use to determine whether it is appropriate and permissible to sell, lease, or otherwise profit from biometric data. Alternatively, companies may opt to implement a blanket prohibition on any type of selling or leasing of biometric data to mitigate potential liability exposure.

Data Security Measures

- [ ] Implement data security safeguards to protect all biometric data captured, used, possessed, and stored by the company from improper disclosure, access, or acquisition.
- [ ] Data security measures should, at a minimum, protect biometric data:
- [ ] using the reasonable standard of care applicable to the company's given industry; and
- [ ] in a manner that is the same or more protective than the manner in which the company stores, transmits, and protects other forms of sensitive personal information.

Vendor Management

- [ ] Strive to manage risk to the greatest extent possible as it relates to vendors and other service providers that supply the technology used to process and store biometric data.
- [ ] Before entering into a relationship with a vendor that will have access to biometric data, perform necessary due diligence and vetting to ensure that the vendor's security measures are sufficiently robust.

  Comment: Key due diligence areas include: (1) implementation and maintenance of comprehensive, up-to-date security policies and incident response plans; (2) performance of regular penetration testing and security audits; and (3) completion of background checks on all vendor employees and other individuals who will be given access to biometric data.
- [ ] Review and update contracts with vendors to address issues raised by biometric privacy laws.
- [ ] Key contractual provisions include:
  - [ ] Prohibition on the disclosure or sale of biometric data.
  - [ ] Compliance with laws.
  - [ ] Minimum data security standards.
  - [ ] Security incident standards, cooperation, and reimbursement of remediation expenses.
  - [ ] Audit rights.
  - [ ] Indemnification.
- [ ] Ensure that vendors and service providers continue to maintain sufficient security safeguards over time through ongoing monitoring and audits.

Arbitration Agreements & Class Action Waivers

- [ ] Consider use of arbitration agreements and class action waivers to limit potential exposure.

  Comment: Companies that do not currently have arbitration provisions and class action waivers in their contracts and agreements, such as Terms of Use and employment agreements, should work closely with experienced biometric privacy counsel to revise their contracts/agreements to include this key tool. Companies whose contracts/agreements currently contain arbitration provisions and class action waivers should evaluate the efficacy of their existing contracts/agreements to avoid any unexpected pitfalls resulting from improper or outdated language or failing to adhere to current requirements relating to the enforceability of arbitration agreements.
- [ ] Drafting considerations:
  - [ ] Provide notice at the beginning of the agreement that highlights the inclusion of an arbitration provision.
  - [ ] Place the arbitration provision itself clearly and conspicuously at the beginning of the agreement.

☐ Incorporate the use of broad language to ensure the arbitration provision encompasses any potential claims or disputes that may arise out of the collection and/or use of biometric data and any laws implicating the use of biometrics.

☐ Where applicable, specify that the Federal Arbitration Act ("FAA") and federal arbitration law applies to the issue of arbitration, describe what arbitration entails, and explain the rights the individual is relinquishing by agreeing to arbitration.

☐ Specify that "gateway" issues, such as disputes about arbitrability—or, in other words, whether the parties agreed to arbitrate a dispute—will also be decided by an arbitrator, and not a court.

☐ Ensure all class action waivers include explicit language making clear that—in addition to precluding class action litigation—class arbitration is also barred under the agreement, in order to remove any doubt that arbitration must be conducted on an individual basis.

Unionized Employers: Collective Bargaining Agreements (CBAs)

☐ Review CBAs to ensure they address the collection and use of biometric data from unionized employees.

☐ Review CBAs to ensure they address the issues of notice and consent as it relates to the collection and use of biometric data.

Comment: Companies with unionized employees may have the ability to use a preemption defense, forcing unionized workers to resolve all biometric disputes through the grievance process described in the CBA.

To avail themselves of the defense, companies should provide unequivocal, advance notice to union representatives regarding the intent to collect and use employee biometric data for business purposes. Notice should be conveyed not only during the collective bargaining process, but also in the terms of the CBA itself. Companies should ensure that the CBA contains unequivocal language stating that the union has consented to the collection and use of its members' biometric data for business purposes.

