BARACK FERRAZZANO

Barack Ferrazzano Kirschbaum & Nagelberg LLP

UPDATED: FEBRUARY 2019

# BIOMETRIC INFORMATION PRIVACY LAWS IN THE UNITED STATES: COMPLIANCE CHECKLIST

***NOTE:** Currently, three states have biometric data privacy laws, though only Illinois provides a private right of action.[1] This is a fast-evolving area, however, and other states may pass similar laws.[2] This checklist includes requirements common to the three laws, and, where requirements vary, incorporates the more protective approach. It is important to consult with an attorney for project-specific implementation and advice.*

The Biometric Data Privacy Compliance Checklist is a supplement to our *Client Alert*: https://www.bfkn.com/ca_201902_BIPA

1. **Biometric Identifier:** If a person's biometric identifier or information is involved, a Company must have a:
   - ☐ Written policy:
     - ○ That is available to the public
     - ○ Detailing the retention and destruction of the information

     NOTE: The company must follow its policy unless a court orders otherwise.

2. **Collection:** Before collecting, capturing, purchasing, or receiving a person's biometric identifier or information, a Company must:
   - ☐ Inform the person (or the person's legal representative, such as a parent) in writing:
     - ○ That the person's biometric identifier or biometric information is being collected or stored; and
     - ○ Provide the specific purpose and length of time for which the biometric identifier or biometric information is being collected, stored, and used

   - AND -
   - ☐ Obtain a written release signed by the person (or the person's legal representative, such as a parent)

3. **Disclosure:** Before disclosing or otherwise sharing a person's biometric identifier or information, a Company must:
   - ☐ Obtain written consent from the person (or the person's legal representative, such as a parent)

     NOTE: Written consent for collection and storage can be obtained at the same time as consent for disclosure. Certain exceptions to consent may apply, such as when disclosure is required by law or by a subpoena, or where disclosure completes a financial transaction requested by the person.

1 These include Texas (Tex. Bus. & Com. Code Ann. § 503.001, *et seq.*), Washington (Wash. Rev. Code Ann. § 19.375.010, *et seq.*), and Illinois (740 ILCS 14/15, *et seq.*).

2 Additionally, more general data privacy laws could be implicated by biometric information collection and storage. These include, for example, state data breach notification laws or industry-specific regulations (such as healthcare).


UPDATED: FEBRUARY 2019

## BIOMETRIC INFORMATION PRIVACY LAWS IN THE UNITED STATES: COMPLIANCE CHECKLIST *(cont'd.)*

4. **Retention/Storage:** A Company is required to:
   - ☐ Store, transmit, and protect all biometric identifiers and information from disclosure using the reasonable standard of care within the industry

     NOTE: The retention and storage must be in a manner that is at least as protective as the manner the Company treats other confidential and sensitive information (such as account numbers, PIN numbers, etc.).

5. **Permanently Destroy:** A Company must permanently destroy biometric identifiers and information by (whichever occurs soonest):
   - ☐ When the initial purpose for collecting or obtaining such information has been satisfied

     - OR -
   - ☐ Within 3 years of the individual's last interaction with the private entity

6. **Not for Sale:** A Company cannot sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or information.