SHOOK
HARDY & BACON

Hot Topics in Privacy and Data Security Law

Erin Hines, Of Counsel
Dan Rohner, Of Counsel
Al Saikali, Partner
Shook, Hardy & Bacon, LLP

James Theiss
Sr. Corporate Counsel
Privacy & Security
DaVita, Inc.

Agenda

1. Colorado Data Breach Notification Law
2. Biometric Privacy Laws (BIPA)
3. California Consumer Privacy Act
4. Other Legislative Developments

Colorado Privacy Law

What did H.B. 18-1128 require?

- Amends the state's data breach notification law to require notice to affected Colorado residents and the Colorado Attorney General within **30 days** of determining that a security breach occurred;
- Imposes **content requirements** for the notice to residents;
- Expands the **definition of personal information**;
- Establishes **data security requirements** applicable to businesses and their third-party service providers; and
- Amends the state's law regarding **disposal of personal information**.

How do I minimize my risks?

- Prepare an incident response **plan**
- Engage your incident response **vendors** now (consider cyber liability insurance)
- Perform a **tabletop exercise**
- Perform a **data inventory**
- Consider a third-party information security **assessment**

Biometric Privacy

What is a Biometric Identifier?

Biometric identifier: "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."

Expressly does ***not*** include:

- Writing samples
- Written signatures
- Photographs
- Human biological samples used for valid scientific testing or screening
- Demographic information
- Tattoo descriptions
- Physical descriptions (*e.g.* height, weight)
- Certain information under the Illinois Anatomical Gift Act, the Genetic Information Privacy Act, and HIPAA.

What is Biometric Information?

Biometric information: Any information, regardless of how captured, converted or stored "based on an individual's biometric identifier used to identify an individual."

How Does it Work?

- Scan measures ridge patterns or “minutiae points.”
- An algorithm is applied to create a mathematical representation of the person.
- The numerical representation is encrypted/stored, and sometimes associated with another piece of information, like an employee number or badge number.
- Cannot be reverse engineered.
- No images are stored long-term.

How "Biometric" Technology is Marketed

- Authentication for facility access
- Customer Identification
- Workplace – time-keeping
- Public safety (surveillance, facial recognition)

U.S. Biometric Information Laws

Biometric Information Privacy Laws

- California*
- Illinois
- New York*
- Texas
- Washington

Proposed legislation

- Florida
- Massachusetts*
- Michigan
- New Hampshire*
- New Jersey
- New York

Biometric Data is "PI" (State Breach Notification Laws)

- Delaware
- Illinois
- Iowa
- Maryland
- Nebraska
- New Mexico
- South Dakota
- Wisconsin
- Wyoming

* Not materially the same as Illinois BIPA

State Law Comparison

	Illinois	Texas	Washington
Private Right of Action?	Yes	No	No
Available Relief?	$1,000 / negligent violation $5,000 / reckless violation Injunction, costs, fees No max liability in statute	$25,000 / violation (max)	$500,000 (max)
Scope Limited to Commercial Purposes?	No	Maybe	Yes
Sale Permitted?	No	Sometimes	Sometimes
Rules for Notice, Consent, Disclosure, Retention, and Destruction?	Yes	Yes	Yes

Typical Requirements

- Applicable to **private entities**;
- Require **notice** and **consent/release** before biometric information is collected;
- **Limit the sale and disclosure**;
- Require **reasonable care** to safeguard;
- **Limit retention** to the purpose for its collection; and
- Require **destruction** when no longer needed.

The BIPA Private Right of Action

"Any **person aggrieved** by a violation of [BIPA] shall have a right of action," and "a prevailing party may recover **for each violation**."

- $1,000 (negligence) / $5,000 (intentional)
- Attorneys fees; costs; injunctive relief

Defenses for Employers

- Individual arbitration agreements
- Workers' Compensation Act
- Unionized workforce
- Reduced expectation of privacy
- "Financial transaction" under BIPA
- Labor law preemption
- HIPAA preemption

The Storm Ahead: California Consumer Privacy Act

SHOOK
HARDY & BACON

Who does it apply to?

- For-profit entities that do business in CA;
- Collect, sell, or disclose **personal information** of California **consumers**;
- Determine the purposes and means of processing;
- The business does any of the following:
  - Generates annual gross revenue > $25M;
  - Has PI for 50k or more consumers; or,
  - Derives 50% or more revenue from sale of PI.

"Personal Information"

- "*Personal Information*" is information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household

Examples of "Personal Information"

1. **Identifiers** such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

2. Any categories of personal information described in the CA **breach notification law.**

3. Characteristics of **protected classifications** under California or federal law.

4. **Commercial information**, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

5. **Biometric information**.

6. **Internet or other electronic network activity information**, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

More Examples of "Personal Information"

7. **Geolocation** data.

8. **Audio, electronic, visual, thermal, olfactory**, or similar information.

9. Professional or **employment-related information**.

10. **Education information** that is not publicly available.

11. **Inferences** drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

What does it do?

1. **Right to know** about privacy practices
2. **Right to access** personal information
3. **Right to delete** personal information
4. Requires **opt-in for sale of minors' PI**
5. Right to **opt out of the sale of information**
6. **Right against discrimination** (maybe consent for *loyalty programs*)
7. **Right to sue** for data breaches

When does the law NOT apply? (1 of 2)

- Complying with other laws
- Complying with a regulatory inquiry, subpoena, or law enforcement
- To exercise or defend legal claims
- Where the personal information is deidentified or aggregated
- If every aspect of the commercial conduct takes place outside CA
- To prevent the violation of an evidentiary privilege

When does the law NOT apply? (2 of 2)

- PHI collected by a CE or BA under HIPAA/HITECH
- Medical information governed by the California Confidentiality of Medical Information Act
- Info collected as part of a clinical trial under federal law
- Sale of PI to/from a consumer reporting agency if used to generate a consumer report under the FCRA
- PI collected, processed, or disclosed under the GLBA, the CA Financial Info Privacy Act, or the Driver's Privacy Protection Act.

What do you have to do?

1. A **data inventory**
2. Develop a DSAR **intake system**
3. Develop an **opt-out system**
4. Determine **how to "verify"** requests
5. Update **privacy notices/policies**
6. **Train** and implement
7. Amend **service provider contracts**

Random Facts

1. One-year ”look back.”
2. 45 days to respond to DSARs.
3. Right to delete exceptions swallow rule.
4. Kids ages 13 to 15 don’t need parental consent.
5. Safe harbor from liability for service provider if you update contract.
6. Right to cure for PRA is meaningless.

Enforcement – penalties; timing

- The AG can impose fines of up to **$2,500 for each violation** of the CCPA or up to **$7,500 per each intentional violation.**

- The AG's ability to bring enforcement actions begins six months after publication of the implementing regulations or July 1, 2020, whichever comes first.

2019 Amendments

- **SB 561** – creates private right of action for privacy violations; removes right to cure for AG enforcement.
- **AB 25** – amends definition of "consumer"
- **AB 846** – clarifies that consumers are not prohibited under the CCPA from choosing to participate in customer loyalty programs that offer incentives such as rewards, gift cards, or other benefits.
- **AB 1202** – data brokers must register and provide information to the CA Attorney General's office.
- **AB 950** – companies must publicly post the average monetary value of a consumer's data on their website.

Legislative Activity

Florida (SB 1270) and NY (SB 1203) considering BIPA

- Identical to Illinois BIPA
- Would include private rights of action

States Considering Privacy Laws

- Connecticut (SB 1108)
- Hawaii (SB 418)
- Maryland (SB 613)
- **Massachusetts (SB 120)**
- Mississippi (HB 1253) (failed)
- **Nevada (SB 220)**
- New Mexico (SB 176)
- **New York (SB S224)**
- North Dakota (HB 1485)
- Rhode Island (S 234)
- **Washington (SB 5376)**

Congress Considering a Federal Data Privacy Law

- Contours still not clear
- Who will enforce it?
- Will it preempt state laws?
- Will it have a private right of action?

SHOOK
HARDY & BACON

THANK YOU!

Erin Hines, Of Counsel
Dan Rohner, Of Counsel
Al Saikali, Partner
Shook, Hardy & Bacon, LLP

James Theiss
Sr. Corporate Counsel
Privacy & Security
DaVita, Inc.