U.S. States Privacy Buffet

Too Much To Digest……?
As security risks to citizens' personally identifiable information have increased in recent years, some state legislatures are taking a more active role to require that businesses protect personal information.

State-level momentum for comprehensive privacy bills is at an all-time high. After the California Consumer Privacy Act passed in 2018, multiple states proposed similar legislation to protect consumers in their states.
At least 25 states have laws that address data security practices of private sector entities.

Most of these data security laws require businesses that own, license, or maintain personal information about a resident of that state to implement and maintain "reasonable security procedures and practices" appropriate to the nature of the information and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. In addition to the laws listed later in this presentation, states also have other data security laws that apply to state agencies or other governmental entities.
Let’s Get Educated So We Know What’s On Our Plate…

The number of states with these types of data security laws has **doubled since 2016**, reflecting growing concerns about computer crimes and breaches of personal information.

This session is to help navigate which States “laws” are actually passed, which ones are still in limbo, and what are the common criteria for compliance between them all.

Sifting through the Buffet options to find something healthy and appropriate is what we’re looking to walk away with from this session.
State Data Security Laws over 2 Years…
State Comprehensive- Privacy Law Comparison…

1. Hawaii SB 418 is pending while the task force has been adopted.

2. Maine LD 946 applies only to internet service providers.

3. New York SB S5642 includes a broad consumer right to opt-out of any processing, not just the sale of personal information.

4. Texas HB 4390 is a GDPR-style restriction-based bill that prohibits a business from collecting or processing information except under certain circumstances.
Consumer Rights vs. Business Obligations

- Access to Collected Data
- Access to Shared Data
- To Rectification To Deletion of Data
- To Restriction
- To Portability
- To Opt-Out Against Solely Automated Decision Making
- Private Right of Action

- Strict Age-based Opt-In
- Notice/Transparency Requirement
- Data Breach Notification
- Risk Assessment
- Prohibition on Discrimination
- Purpose Limitation
- Processing Limitation
- Fiduciary Duty
Consumer Privacy Provisions Explained…

- **The right of access to personal information collected** — The right for a consumer to access from a business/data controller the information collected or categories of information collected about the consumer; right may only exist if a business sells information to a third party.

- **The right of access to personal information shared with a third party** — The right for a consumer to access personal information shared with third parties.

- **The right to rectification** — The right for a consumer to request that incorrect or outdated personal information be corrected but not deleted.

- **The right to deletion** — The right for a consumer to request deletion of personal information about the consumer under certain conditions.

- **The right to restriction of processing** — The right for a consumer to restrict a business's ability to process personal information about the consumer.

- **The right to data portability** — The right for a consumer to request personal information about the consumer be disclosed in a common file format.

- **The right to opt out of the sale of personal information** — The right for a consumer to opt out of the sale of personal information about the consumer to third parties.

- **The right against solely automated decision making** — A prohibition against a business making decisions about a consumer based solely on an automated process without human input.

- **A consumer private right of action** — The right for a consumer to seek civil damages from a business for violations of a statute.
### Business Obligations for Privacy Data Sets Explained…

<table>
<thead>
<tr>
<th>Obligation Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A strict opt-in for the sale of personal information of a consumer less than a certain age</strong></td>
<td>A restriction placed on a business to treat consumers under a certain age with an opt-in default for the sale of their personal information.</td>
</tr>
<tr>
<td><strong>Notice/transparency requirements</strong></td>
<td>An obligation placed on a business to provide notice to consumers about certain data practices, privacy operations, and/or privacy programs.</td>
</tr>
<tr>
<td><strong>Data breach notification</strong></td>
<td>An obligation placed on a business to notify consumers and/or enforcement authorities about a privacy or security breach.</td>
</tr>
<tr>
<td><strong>Mandated risk assessment</strong></td>
<td>An obligation placed on a business to conduct formal risk assessments of privacy and/or security projects or procedures.</td>
</tr>
<tr>
<td><strong>A prohibition on discrimination against a consumer for exercising a right</strong></td>
<td>A prohibition against a business treating a consumer who exercises a consumer right differently than a consumer who does not exercise a right.</td>
</tr>
<tr>
<td><strong>A purpose limitation</strong></td>
<td>An EU General Data Protection Regulation–style restrictive structure that prohibits the collection of personal information except for a specific purpose.</td>
</tr>
<tr>
<td><strong>A processing limitation</strong></td>
<td>A GDPR-style restrictive structure that prohibits the processing of personal information except for a specific purpose.</td>
</tr>
<tr>
<td><strong>Fiduciary duty</strong></td>
<td>An obligation imposed on a business/controller to exercise the duties of care, loyalty, and confidentiality (or similar) and act in the best interest of the consumer.</td>
</tr>
</tbody>
</table>
Privacy Challenges When Left to the States…

Reauthorizing the USA FREEDOM Act of 2015
Wednesday, November 6, 2019

State Breach Notifications Calling Themselves Privacy Laws

© NCC Group 2019. All rights reserved
Privacy Challenges When Left to the States…

| • There is no US Constitutional Right or Guarantee of Privacy for US Citizens. | • Given the lack of a Federal Privacy Standards similar to GDPR, PIPEDA, CSL, Japanese san-sho-san (4 Pillars) there is not a congruent baseline to base these user privacy laws off of. |
| • However, the Supreme Court has found that the Constitution implicitly grants a right to “privacy” against governmental intrusion from the First Amendment, Third Amendment, Fourth Amendment, and the Fifth Amendment. The Constitutional concept of privacy uses the theory of natural rights, and generally applied to the new informational age and communication technologies. | • Who’s a citizen of what State? When? Where? Why? What are the metrics a state will use to determine that? Most of us don’t live where we were born. |
| • Without a set of basic and commonly legislated answers to what rights a US Citizen is owed, any implementations that we add to suffice a State Data Privacy requirement could easily disrupt trade, the ability to do business globally. | • An Assumed Approach is all that can be used as a baseline, to help build and maintain "reasonable security procedures and practices" |
| • It is important to first and foremost understand if the state’s privacy law even applies to your organization or client’s entities. In some cases it’s just a simple addendum to an existing policy or procedure to take your compliance and make it applicable to a another requirement. | • Of course, yet ironically, state governments hold a vast amount of data about citizens, including personally identifiable information such as Social Security numbers, driver’s license information, and tax and financial information. |
| • All states have security measures in place to protect data and systems. However, as listed below, at least 29 states require--by statute--that state government agencies have security measures in place to ensure the security of the data they hold. Many of these laws have been enacted in just the past two to three years, as cybersecurity threats and attacks against government have increased. |
Data Protection in the United States

When data privacy was first established in the European Union, it was a potpourri of industry-specific protections. Unfortunately, the United States never moved past this stage, and the current data privacy climate is itself a hodgepodge of laws passed when specific industries required them.

In fact, the goal of US privacy law appears to be more focused on the efficiency of data flow rather than the sum-total protection of private data from unauthorized use and access.

In general terms, in the U.S., whoever can be troubled to key in the data, is deemed to own the right to store and use it, even if the data were collected without permission. For instance the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Children’s Online Privacy Protection Act of 1998 (COPPA), and the Fair and Accurate Credit Transactions Act of 2003 (FACTA), are all examples of U.S. federal laws with provisions which tend to promote information flow efficiencies.

Though several significant attempts have been made to establish the privacy of an individual’s data, these attempts are largely industry-specific. The aforementioned Health Insurance Portability and Accountability Act (HIPPA), for example, specifically establishes procedures for health information collection, disclosure, use, and the inherent rights therein.

Likewise, the Electronic Communications Privacy Act (ECPA) attempted to establish certain protections of private data over electronic communication systems; unfortunately, the large amount of loopholes therein renders the rights null, as consent can be given either directly, as in the case of a data request, or implicitly, as when an employee uses email that is then monitored by their company.
So Where Do we go from here?

KEEP CALM AND USE LOGIC
**The Approach**

In order to effectively comply with new States’ Data Privacy obligations, businesses need to be able to prove where any of their client’s (or potential clients’) personal information is located. Additionally, the organization has the onus of responsibility to prove knowledge, as well as how it is being processed, shared and stored.

Businesses falling within the State’s Data Privacy Sets scope should consider the following approach to help understand the scope of their responsibilities:

- Executive States’ Data Privacy Awareness workshop
- **Data discovery & mapping** (to formulate a records of processing)
- Privacy Risk Screening (PRS)
- Data Protection Impact Assessment (DPIA) or Privacy Impact Assessment (as some standards refer to it as)
- Privacy Data Set Health/ Compliance Check
  - Compliance index (dashboard) based on States’ Data Privacy Legislation
  - Detailed findings and recommendations
  - Privacy notices, opt-in/opt-out processes, minor children procedures, breach assessments/notification, and request handling/tracking
The Approach (cont’d)

<table>
<thead>
<tr>
<th>Interviews</th>
<th>Document review: Key documents (including):</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of interviewees:</td>
<td></td>
</tr>
<tr>
<td>● People responsible for Governance</td>
<td>● Supplier manager</td>
</tr>
<tr>
<td>● Person responsible for Physical Security</td>
<td>● Senior HR person</td>
</tr>
<tr>
<td>● Person responsible for Information Security</td>
<td>● Person responsible for contracts</td>
</tr>
<tr>
<td>● Person responsible for IT change control</td>
<td>● Person responsible for Risk</td>
</tr>
<tr>
<td>● Person responsible for System Administration</td>
<td>● Person responsible for Operational Management</td>
</tr>
<tr>
<td>● Senior procurement person</td>
<td></td>
</tr>
</tbody>
</table>

- Organizational chart showing governance bodies
- Details of any privacy-related training given to employees
- Policies and procedures
- Privacy notices
- IT change control process
- Joiners, movers and leavers procedure(s)
- Data Breach Policy and Process (including response templates)
- Data Processor documentation (Governance and Compliance Checklists)
- Material relating to the management of subject access requests (Policy, process and template responses)
- Records of consent given by customers or clients
- Data Inventory (listing data held and location)
- Examples of all standard contracts for third parties (can be templates)

- **Corporate risk register**
Thank You.

Q&A