Privacy Trends in the US and Implications for US and Global Organizations

September 15, 18th Annual CEI
National Harbor, MD

Disclaimer: The handouts for this presentation were prepared and used to accompany this session. Neither the information contained herein or the accompanying comments of the presenter should be construed as the provision of legal advice. Views expressed are those of the specific presenter.
Outline

01 Baselining: What is Privacy?
02 Update on the State of US Consumer Privacy Laws and Bills
03 Understanding Trends and Themes
04 How to “Future-Proof” Your Privacy Compliance Initiatives

What is Privacy?
### Baselining: How Do We Define Privacy?

- Right to be left alone?
- Information privacy?
- The world we want to live in?

### Compliance, Privacy and Security

<table>
<thead>
<tr>
<th>Compliance</th>
<th>Data (Information) Privacy</th>
<th>Data Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>A systematic approach to governance designed to ensure that an organization meets its obligations under applicable laws, regulations, best practices, contracts, and internal policies.</td>
<td>Generally focused on the use and governance of PII. Organizations must implement policies to ensure that personal information is being collected, shared, and used in appropriate ways.</td>
<td>Focuses on protecting data (PII, confidential information, etc.) from impermissible access, including intentional malicious attacks. Organizations maintain the privacy of their data by having security protocols in place to prevent against external threats and data breaches.</td>
</tr>
</tbody>
</table>
The US Consumer Privacy Laws and Bills
Overview of existing and pending legislation and requirements

The US Consumer Privacy Laws and Bills
Pending and Adopted Legislation
California Consumer Privacy Act - Overview

- Stated to go into effect January 1, 2020
- Set to be one of the toughest privacy laws in the US
  - New states already passing similar bills
- Broadly expands the rights of consumers
  - Requires in scope businesses to be more transparent about collection, use, disclosure and sale of personal information
- May be a motivating event for businesses to enhance data privacy management practices
- For companies subject to GDPR, ability to leverage GDPR initiatives to address operational needs

Who must comply?

- Any business worldwide doing business in California;
- Exceeding thresholds of:
  - Annual gross revenues of $25 million;
  - Personal information of 50,000 or more California residents, households, or devices annually; or
  - 50% or more annual revenue from selling California residents’ personal information.
- Parent companies and subsidiaries sharing the same branding, even if they themselves do not exceed the applicable thresholds
Who must comply? Key Definitions

Personal Information
- Any information associated with, relating to, or capable of being associated with, or that could reasonably be linked, directly or indirectly, with a particular consumer or household.
  - See § 1798.140(o).

Consumer
- A natural person who is a California resident.
  - See § 1798.140(g).

Sale
- Selling, renting, releasing, disclosing, transferring, making available, or otherwise communicating a consumer’s personal information to another business or a third party for monetary or other valuable consideration.
  - See § 1798.140(t).

Business
- Any for-profit entity that collects personal information, determines the purposes and means of processing that information, does business in California, and meets at least one threshold related to revenue or volume of personal information collection; and
  - Any entity that controls, or is controlled by, a qualifying business if it shares common branding.
  - See § 1798.140(c).

Service Provider
- Any for-profit entity that: (1) processes personal information on behalf of a business (2) pursuant to a written contract that prohibits the service provider from retaining, using, and disclosing personal information other than for the specific purpose of performing the service specified in the contract or as CCPA otherwise allows.
  - See § 1798.140(v).

Third Party
- Defined in the negative to include any person other than: (1) the business that collects consumer personal information; or (2) a person who receives personal information from a business pursuant to certain contractual limitations (similar to restrictions imposed on service providers).
  - See § 1798.140(w).
Main Individual Rights

1. RIGHT OF ACCESS
2. RIGHT OF DELETION
3. RIGHT TO DATA PORTIBILITY
4. RIGHT TO INFORMATION ON DATA SELLING
5. RIGHT TO OPT-OUT OF DATA SELLING
   6. DO NOT SELL BUTTON/LINK
7. PRIVATE RIGHT OF ACTION (breaches)

Rights mainly apply to data collected in the 12 months preceding the request and can be exercised free of charge.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

- Applies in the State of California and to organizations doing business there
- Legislation focuses on data subject rights
- Rights only extended to California residents
- Will apply as of 1 January 2020; changes to the body of law still possible

How to comply?

Update Privacy Policies:

- Provide at or before collection: categories of personal information (PI) to be collected and underlying purposes (information may be provided elsewhere)
- Separate lists of categories of PI collected, sold or disclosed for a business purpose in the preceding 12 months (explicitly state if not sold or disclosed)
- Categories of sources of PI collected
- Business/commercial purposes for collecting or selling PI
How to comply?

Update Privacy Policies to Include:

- Categories of third parties receiving PI
- Description of the rights to access, deletion, to obtain information about disclosures, to opt out of sales, and not to be discriminated against
- If PI is sold: Fact that PI collected may be sold and clear and conspicuous link, titled "Do Not Sell My Personal Information", to webpage that enables opt-out
- Method(s) for submitting requests including, at a minimum, toll-free telephone number and, where maintained by the business, website address

How to comply?

A business shall not discriminate against a consumer because the consumer exercised any of the consumer’s rights under this title, including, but not limited to, by:

a) Denying goods or services to the consumer.
b) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
c) Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer’s rights under this title.
d) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.
How to comply?

Access, Deletion rights: Implement processes and policies to

- verify the identity of individuals making requests
- timely provide portable copies
- delete personal information or claim statutory exception

(1) Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Detect security incidents, protect against malice, theft, fraud, or illegal activity, or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencement with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws when the business' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(8) Comply with a legal obligation.

(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

- obtain assistance of service providers
Nevada
Main Individual Rights

1. **RIGHT TO OPT-OUT OF DATA SELLING**
2. **DO NOT SELL BUTTON/LINK**

Amends an existing online privacy notice law and is significantly narrower than the CCPA. Sale of data more narrowly defined: exchanging personal information specifically for monetary consideration and for onward licensing or sale.

### ACT RELATING TO INTERNET PRIVACY

- Applies to “operators” (≠ business)
- Defines consumer in more limited way
- Does not extend to household information
- Legislation focuses on sale of data
- Rights only extended to Nevada residents
- Will apply as of 1 October 2019
The US Consumer Privacy Laws and Bills
Pending and Adopted Legislation

- California
- Louisiana
- Maine
- Maryland
- Massachusetts
- Minnesota
- Nevada
- New Jersey
- New York
- Pennsylvania
- Puerto Rico
- Vermont
- Washington

Understanding Trends and Themes
The US Consumer Privacy Laws and Bills

Parallels

**“DO NOT SELL” PERSONAL INFORMATION**
- Individual can request information about data sales
- Individual has the right to opt-out of data sales
- Organization has the obligation to display opt-out link or button

**GDPR AND CCPA-LIKE RIGHTS & OBLIGATIONS**
- Individual has the right of access to his/her data
- Individual can request correction or deletion of data

**STRONG ENFORCEMENT**
- Attorneys-General in charge of enforcement
- Possibility to impose penalties or hold organizations liable

**EQUAL TREATMENT**
- Prohibition to discriminate against consumers exercising their rights

---

The US Consumer Privacy Laws and Bills

Differences

**SCOPE OF APPLICATION**
- Significant differences between jurisdictions
- Depending on annual gross revenue, number of consumers, etc.
- Covered data: e.g. employee data, healthcare data not consistently covered

**PRIVATE RIGHT OF ACTION**
- Only included in some of the bills, unlike CCPA or GDPR
- Notable examples are Louisiana, Maryland, Massachusetts, New York, Pennsylvania, Puerto Rico and Washington

**ACCOUNTABILITY**
- Significant differences between jurisdictions on requirements to be able to demonstrate compliance
The US Consumer Privacy Laws and Bills

Outliers

Maine
Maine - SB946 (law)
(Providers of broadband Internet access services)

Louisiana
Louisiana - HB465 (bill)
(Providers of broadband Internet access services)

Puerto Rico
Puerto Rico bill assigns the responsibility for enforcement to the Secretary of Consumer Affairs.

Washington
State of Washington bill includes limits to the use of facial recognition:
meaningful human review, consent, court order needed when surveilling specific individuals.

It follows the more extensive structure of the GDPR and includes definitions of sensitive data, controller and data subjects and requires transparency.

Unlikely to be discussed before 2020.

Federal Law
How to Future-Proof Your Privacy Compliance Initiatives: Is It Time to Invest in a Privacy Program?

The Need for a Privacy Program
Main Reasons

- Higher Volume & Continuously Changing Legal Requirements
- Increased Public Awareness
- Increased Enforcement

ACCOUNTABILITY
Accountability

- Globally recognized as a key building block for privacy and data protection regulation
- Gives effect to legal requirements and data privacy laws
- Delivers corporate digital responsibility for the 21st century and modern, data-driven economies
What must organizations do to be “accountable”?

Accountability requires organizations to:

• Implement within the company a comprehensive privacy program covering all core elements of accountability that enables compliance with applicable laws, regulations or industry standards
• Verify the effectiveness and delivery of such a privacy program and ensure continuous improvement
• Be able to demonstrate the existence and effectiveness of such a program internally (to Board and senior level management) and externally on request (to regulators, business partners and individuals)
Traditional Compliance Assessment Approach

Many Regulatory Requirements  to  Many Privacy Programs & Activities

- EU GDPR
  - Rule 1
  - Rule 2
  - Rule 3
  - Rule 4
  - Rule 5

- Brazil LGPD
  - Rule 1
  - Rule 2
  - Rule 3
  - Rule 4
  - Rule 5

- California CCPA
  - Rule 1
  - Rule 2
  - Rule 3
  - Rule 4
  - Rule 5

- Hong Kong Ordinance
  - Rule 1
  - Rule 2
  - Rule 3
  - Rule 4
  - Rule 5

- Mexico Data Protection Act
  - Rule 1
  - Rule 2
  - Rule 3
  - Rule 4
  - Rule 5

- PHI Policies & Procedures

- Training and Awareness

- Human Resources

- Legal

- Vendor Management

Rationalized Rule Set

- Rule A
- Rule B
- Rule C
- Rule D
- Rule E
Accountability Based Approach
Leverage existing activities to comply with many laws and evidence of accountability to demonstrate compliance

ONE ACCOUNTABLE PRIVACY PROGRAM
Evidence of Privacy Management Activities exists throughout the organization (within the privacy program as well as operations). Evidence is collected in centralized repository, structured in a line with the Privacy Management "categories."

MANY REGULATORY REQUIREMENTS
Evidence of accountability is mapped to requirements, allowing the organization to demonstrate compliance with laws and regulations on-demand, supported by evidence.

Accountability Approach to Compliance with Multiple Laws

ACCOUNTABILITY
Privacy Programme Infrastructure
- Responsibility
- Ownership
- Evidence

CAPACITY TO COMPLY
Privacy Programme Outcomes
- Laws and regulations (LGPD, GDPR, California CCPA and 800 other privacy laws and regulations)
- Regulator Guidance
- Enforcement Actions
- Codes

How does the organization comply?

Can the organization demonstrate a capacity to comply?
Nymity Privacy Management Accountability Framework
ISO 27701 (Formerly 27552)
Enhancement to ISO/IEC 27001 for Privacy Management

- To enhance the existing Information Security Management System (ISMS) with additional requirements in order to establish, implement, maintain, and continually improve a Privacy Information Management System (PIMS)
- Outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage privacy controls to reduce the risk to the privacy rights of individuals
- Intended to be a certifiable extension to ISO/IEC 27001 certifications