Changing Legal Landscape: Privacy Developments

Jennifer Urban Rathburn, Partner
Foley & Lardner LLP
The Legal Landscape Affecting Insurance Companies is Changing

- As many scholars debate the merits of a comprehensive legal privacy regime versus allowing industries and companies to self-regulate, the strong trend has been toward more sweeping privacy legislation at the international, federal, and state levels.

- For example, New York State’s cybersecurity regulation for financial services companies (23 NYCRR 500), the EU’s General Data Protection Regulation (GDPR), Nevada’s privacy law, and the California Consumer Privacy Act (CCPA) have all been enacted in the last five years.
  - Comprehensive laws in many other state and federal jurisdictions are on the horizon (e.g., Washington’s reintroduced privacy bill and the federal privacy bill known as COPRA).
  - While many new laws exempt large swaths of personal information related to insurance companies (e.g., the CCPA carves out GLBA and the California Financial Information Privacy Act covered data), these exemptions are often limited to the specific data, not the business itself.
“Where does the insurance industry fit within emerging privacy regimes given GLBA and state insurance laws?”
Regardless of Your Legal Coverage, Investing in Privacy is a Smart Business Decision from an ROI Perspective

- Consumers are increasingly expecting businesses to not only be transparent about their data practices, but to provide greater choices to individuals about how their data is used and shared.
  - Having a strong privacy program can create a strong competitive edge.
  - A recent study from Cisco found that for every $1 an organization spends on privacy, they receive a $2.70 return on investment.
As New Legal Regimes Emerge, There Are Best Practices You Can Do to Prepare for Compliance

Know your data

Review and update policies

Processes and mechanisms to respond to individual rights

Update third-party contracts where PI is shared

COMPLIANCE
Know Your Data

- **WHO**
  - Has access?
  - Does the data pertain to?

- **WHAT**
  - Types of data?
  - Systems touch the data?

- **WHERE**
  - Is the data stored?
  - Can the data be accessed?
Part of Knowing Your Data is Staying Up-to-Date on Legal Developments

- As you map your data, you can begin to classify it based on the level of protection legal regimes require for it.

- Staying up-to-date on developing laws and regulations will help you classify data based on its sensitivity in regard to the applicable legal requirements.
Implement Processes and Mechanisms to Provide Individuals Privacy Rights

- Develop procedures for processing an individual’s rights under the legal regime, including how to best manage the consent/opt-in/opt-out process, access requests, rights to deletion and related verification responsibilities.
- Develop model consents and a “playbook” for handling requests, and train employees on handling the same.
- Implement technical capabilities to process consumer requests within the required deadlines.
- More on consent . . .
Consent Approach Varies

- Type of Consent
  - Opt-in
  - Opt-out
  - Strict Prohibition: Consent cannot be given

- Determining factors
  - Type of data
  - Purpose of use or disclosure
  - Potential effect is key
  - Numerous data use considerations are emerging re: potential discrimination, denial of a product or service, marketing, sale, differential treatment, AI, use of cookies, geolocation, purchasing habits, ownership, etc.
Review and Update Policies

- Review current policies and practices for any modifications that need to be made based on the new legal regimes that give consumers new rights.
- For example, some laws prohibit discrimination against consumers who exercise their rights or the denial of goods and services based on their privacy choices.
- Other regimes have specific formats or language that must be set forth within privacy notices.
Update Third-Party Contracts Where PI is Shared

- Review and update contracts with third parties and service providers to whom personal information is conveyed to ensure that the other party can appropriately meet the requirements of the legal regime, such as how to respond to consumer requests to access or delete information.

- Review the license you provide to the other party with respect to personal information and data use rights to ensure they comply with applicable law and best practices.

- Determine appropriate, reasonable security measures for the other party.
Questions?