

Assignment 4.1: Analyzing Data Breach Laws and Their Impact

Joshua A. Wortz

University of San Diego

CSOL-540

Dr. Michelle Moore

07/21/2025

Introduction

In an era of increasing cyber threats and data breaches, both state and federal governments have implemented laws to protect consumer data and prevent identity theft. However, these laws differ in scope, enforcement, and effectiveness. This paper compares California's Consumer Privacy Act (CCPA), a landmark state law, with the federal Cybersecurity Information Sharing Act (CISA). By analyzing how each law defines and addresses data breaches, outlines enforcement mechanisms, and provides remedies for non-compliance, this paper evaluates the effectiveness of these frameworks and makes recommendations for improving data breach regulations (Mireles & Hobaugh, 2024).

Key Provisions of the CCPA and CISA

California Consumer Privacy Act (CCPA):

Enacted in 2018 and amended by the California Privacy Rights Act (CPRA), the CCPA grants California residents rights over their data, including the right to know what information is collected, the right to request deletion, the right to opt out of the sale of their data, and the right to hold companies accountable for misuse (California Office of the Attorney General, n.d.). It applies to for-profit businesses that meet thresholds related to revenue, data processing, or the sale of personal data.

Cybersecurity Information Sharing Act (CISA):

Enacted in 2015, CISA focuses on enhancing cybersecurity by facilitating the voluntary sharing of cyber threat indicators between private companies and the federal government (U.S. Congress, 2015). It encourages cooperation by providing liability protections to entities that share

information in good faith, aiming to enhance threat detection and response across sectors (Mireles & Hobaugh, 2024).

How Each Law Defines and Addresses Data Breaches

The CCPA defines a data breach as the unauthorized access, exfiltration, theft, or disclosure of personal information due to inadequate security practices. It ties liability directly to failures in reasonable cybersecurity, allowing consumers to sue for statutory damages if their data is compromised, even without proof of actual harm (California Office of the Attorney General, n.d.).

CISA, in contrast, does not define or directly regulate data breaches. Instead, it facilitates the sharing of “cyber threat indicators” and “defensive measures.” The act's scope is proactive rather than reactive, focused on preventing breaches through shared intelligence rather than punishing mishandling of personal data (U.S. Congress, 2015; Mireles & Hobaugh, 2024).

Enforcement Mechanisms and Penalties for Non-Compliance

The CCPA is enforced by the California Privacy Protection Agency (CPPA) and the California Attorney General. It provides for civil penalties of up to \$2,500 per violation, or \$7,500 for intentional violations. It allows consumers to bring private lawsuits in cases of data breaches involving unencrypted or unredacted personal information (California Office of the Attorney General, n.d.; Mireles & Hobaugh, 2024).

CISA does not impose direct penalties or create enforceable cybersecurity mandates. It is a voluntary compliance framework that incentivizes information sharing by providing liability protections rather than imposing sanctions. CISA lacks an enforcement body, and its

effectiveness depends on voluntary adoption and cooperation from private-sector entities (U.S. Congress, 2015).

Critical Comparison and Effectiveness

State-level laws, such as the CCPA, offer stronger protections for individuals than federal frameworks like CISA. The CCPA's consumer rights, clear breach definitions, and actionable remedies provide concrete legal recourse for those affected by data incidents (California Office of the Attorney General, n.d.). CISA, while necessary for facilitating national-level threat intelligence, lacks enforcement mechanisms and accountability provisions for data mishandling (Mireles & Hobaugh, 2024).

However, the CCPA only protects California residents, highlighting a key limitation of the state-by-state approach. Meanwhile, CISA, while weaker in enforcement, applies broadly to critical infrastructure and encourages collective cybersecurity resilience (YouTube, 2023).

Should There Be a National Law?

A single, comprehensive federal data breach law could reduce confusion and compliance burdens for businesses while ensuring equal protections for consumers across all states.

However, it must be crafted carefully to avoid preempting stronger state laws. A federal baseline that allows states to enact stricter requirements would preserve innovation while promoting national consistency and uniformity (Mireles & Hobaugh, 2024).

Conclusion and Recommendations

To address growing cyber threats effectively, the United States needs a unified data breach regulation framework that combines the strengths of both CCPA and CISA. A comprehensive federal law should:

- Establish minimum consumer rights and breach notification standards.
- Include enforceable security requirements and penalties for non-compliance.
- Preserve the right of states to enhance protections based on local needs.
- Encourage, but not rely solely on, voluntary information sharing.

By merging accountability with collaboration, such a framework would better serve both individuals and businesses navigating today's cybersecurity landscape.

References

Mireles, M. S., & Hobaugh, J. L. (2024). *Cybersecurity and privacy law in a nutshell* (2nd ed.).

West Academic.

YouTube. (2023, June 16). *What do state laws regarding cybercrime generally pertain to...*

[Video]. YouTube. https://youtu.be/4Lw_z-f6wHY

U.S. Congress. (2015). *Cybersecurity Information Sharing Act of 2015*, 6 U.S.C. §§ 1501–1510.

<https://www.congress.gov/bill/114th-congress/senate-bill/754>

California Office of the Attorney General. (n.d.). *California Consumer Privacy Act (CCPA)*.

<https://oag.ca.gov/privacy/ccpa>