Published on *The National Law Review* https://natlawreview.com

Enterprise-Wide Privacy Reality

Article By:

Womble Bond Dickinson Communications, Technology and Media

Our days of stumbling piecemeal toward multiple data privacy and protection standards may be ending.

In the United States, we have seen an increase in calls for a comprehensive federal data privacy law to provide protections, transparency requirements, enforcement powers, and establish enumerated rights for Americans based on the nature of the data collected. As I wrote in October, even business friendly proposals for a federal privacy law integrate these principles. Legislators of different ideologies must jump a significant hurdle: whether to preempt state privacy laws, namely the California Consumer Privacy Act ("CCPA").

A recent IAPP study found that forty-three percent of respondent organizations are complying or in process of complying with two to five data privacy laws. Fifty-six percent of those respondents are working toward a single global data protection strategy. Outside the partisan deadlock, companies are working towards an enterprise-wide privacy solution where companies would offer the same rights and recourse to all their customers regardless of where the consumer resides.

The cost of compliance has increased significantly in the last decade with companies needing to comply with laws, regulations and programs like the GDPR, CCPA, SOX, PCI, and HIPAA. This is particularly true for those companies that are doing business in the United States across sectors and subject to more than one data protection regulation of their activities.

In 1996, HIPAA provided the first American broad, detailed regulations for the use and disclosure of personal health information ("PHI"). The Security Rule of HIPAA requires electronic PHI to be encrypted by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key."

When the Sarbanes-Oxley Act ("SOX"), went into effect in 2002, it sets standards for all U.S. public company boards, management and public accounting firms. Section 302 and 404 of SOX concern protecting data. The combination of encryption and access controls appear essential to safeguarding financial data so that its integrity is assured. Many companies encrypt data regardless of where it resides so that they can guarantee this compliance.

The Payment Card Industry Data Security Standards ("PCI DSS") are security standards set forth by the leading credit card companies through a joint venture. These credit card companies often require

all entities involved in payment processing to comply with these standards. PCI DSS, like SOX and HIPAA stress the need for masking card numbers and encryption of other information.

Despite governing the protection of different types of information (health, financial information, credit card) companies are getting acclimated to responding to consumers, limiting access, and encrypting data. Compliance is no longer a problem for the occasional activist consumer, but a coordinated effort among company employees. A Globalscape whitepaper reveals 32% of compliance costs related to information security comes from direct costs such as payments to consultants, auditors or other outside experts. Simply put – – it is only a matter of time until business practice will cut out the inefficiency of residency-based or vertical-market-based privacy strategies.

Enterprise-wide data privacy strategy may require a significant up-front expenditure and investment as it would lead to data rights being held by consumers who do not currently have them. But companies wll no longer dash toward multiple compliance regimes the way we witnessed in the months preceding the GDPR going into effect, thus saving the administrative costs of sorting out which law supersedes the other. As ideological battles prevent a federal privacy law from taking reality, and the preemption of CCPA takes center stage, companies are working on a future that treats the CCPA and GDPR as if they are already standard.

National Law Review, Volume X, Number 42