Media coverage

USA: Federal privacy framework “would create far greater efficiency”

Breach NotificationData SecurityData TransferLegal Reform

The U.S. Chamber of Commerce ('CoC') released, on 6 September 2018, its Privacy Principles, which provide, among other things, policy recommendations addressed at the U.S. Congress in relation to data privacy ('the Principles').

In particular, the Principles highlight that Congress should adopt a federal privacy framework ('the Framework'), which should include risk-based data security and breach notification provisions, policies that facilitate cross-border data transfers, as well as regulatory safe harbours. In addition, the Principles note that the Framework should not create a private right of action for privacy enforcement since this would divert company resources to litigation that does not protect consumers.

Alan L. Friel, Partner at Baker & Hostetler LLP, told DataGuidance, "The CoC wants one national standard that preempts state and local legislation. The industry pushed hard to avoid the California ballot initiative and keep a private right of action that could open the floodgate of class action lawsuits to a minimum, in what became the California Consumer Privacy Act of 2018. There is concern that other states may follow California and provide broader private rights of action. There is also concern about having to comply with many differing state laws. A single, federal regulatory programme for both privacy and security protection and breach notification would create far greater efficiency than a patchwork of state laws."

The current patchwork quilt of privacy and security laws make compliance difficult, expensive and time consuming, taking businesses away from innovation

The Principles advocate that laws and regulations be flexible and not require businesses to use specific technological solutions or other mechanisms to implement consumer protections. For example, regarding data breach notification, the Principles state that companies should be given flexibility in determining reasonable security practices given that security is different for individual businesses and one-size-fits-all approaches are not effective. Moreover, the Principles note that regulatory safe harbours and similar initiatives would promote the development of adaptable, consumer friendly privacy programmes.

Sandra A. Jeskie, Partner at Duane Morris LLP, noted, "A privacy law that is intended to cover multiple industries, sectors and businesses must by definition allow for businesses to design privacy solutions that address their individual business. Presumably, such a law would provide a minimum set of guidelines with flexibility in implementation to address a broad number of businesses and implementation approaches."

Furthermore, the Principles highlight that businesses should be transparent about the collection, use and sharing of consumer data. They also recognise the importance of privacy innovation, noting that the Framework should encourage stakeholders to consider consumer privacy at every stage of the development of goods and services.

Jeskie concluded, "Whether the Principles are fair to both the interests of companies and consumers depends on where your interests lie. On the one hand, the current patchwork quilt of privacy and security laws make compliance difficult, expensive and time consuming, taking businesses away from innovation. On the other hand, from a consumer perspective, the principles would grant companies significant flexibility in determining appropriate security practices, take away a private right of action from consumers and require that regulators only take enforcement actions against companies when privacy violations result in 'concrete harm to individuals,' a difficult legal standard."

Bart van der Geest Junior Privacy Analyst