



ATTORNEYS AT LAW

12/17/2018 | Insights Tech & Data Insights

Consumer Data Protection Act: The Federal Bill Promising More Protection for Consumer's Data and More Compliance Issues for U.S. Companies

When the European Union (the "EU") passed the General Data Protection Regulation (the "GDPR") in 2016, U.S. companies were not certain whether it would have any ramifications for them. In May, the GDPR went into effect; and most companies, both international and domestic, scrambled to become compliant or assess whether compliance was necessary. We previously have discussed the importance of compliance with the GDPR for domestic companies in various industries and connections. However, the GDPR has had an increasing impact in influencing legislation and inspiring a global trend in stricter data privacy laws.

As previously discussed, the GDPR has inspired bills both internationally (such as India's Privacy Bill) and domestic (including both the California Consumer Privacy Act (the "CCPA") and Colorado's Consumer Data Privacy Law). The domestic state legislation activity directed toward stricter data privacy laws has led to the introduction of a federal bill tentatively titled the Consumer Data Protection Act (the "CDPA"). The CDPA was introduced by Senator Ron Wyden of Oregon in November. Senator Wyden claims the objective of the bill is to prevent companies from profiting from consumer's data. The Federal Trade Commission will enforce the bill and, in so doing, will aim to regulate the collection of consumer data in the following ways:

- submission of annual data protection reports
- power granted to consumers to opt-out of being tracked on websites
- steep fines and criminal penalties for violators

Annual Data Protection Reports

The CDPA will require companies to submit data protection reports to the government. Further, the bill would require top executives of companies, such as their Chief Executive Officers, Chief Operating Officers, etc., to certify the contents of all such reports submitted. The reports must outline the measures taken to ensure the security of all collected personal information and, by certifying those reports, high ranking executives will be held liable for any fraudulent behavior or failure of their companies to comply.

Tracking Opt-Out Provisions

The CDPA will aim to implement a "Do Not Track" tool, which data collecting companies must make available to consumers. The tool will inform service providers that the consumer does not wish to be tracked or have his or her information collected while utilizing their websites, outside of the information voluntarily and expressly given by the consumer to such service providers. This would effectively stop the practice of these service providers collecting consumer data to sell to third-party companies for profit without consent.

Companies such as Facebook have generated outlandish revenues from just such practices for many years. The CDPA acknowledges that the opt-out provision ultimately would destroy a company that generates most of its revenue from dealing consumer data. The bill foresees companies refusing services if an individual opts out of being

tracked. To stop companies from losing profits and to ensure consumers are not discriminated against, the CDPA states that companies are able to charge for what was originally free online services to offset the revenue they will lose by being disabled from tracking and collecting consumer data.

Fines and Criminal Penalties

Similar to the GDPR, the CDPA packs a potent punch. Non-compliance under the bill can result in penalties of up to 4% of a violating company's annual revenue. Unlike the GDPR, the CDPA also targets individual actors and provides for criminal penalties. An executive who knowingly misleads the Federal Trade Commission may be fined up to \$5 million for such misrepresentations and, even more drastically, also could face up to 20 years in prison for such wanton misconduct.

Ramifications for Companies

Currently, the CDPA is in the infancy stage. However, it is reasonable to believe that the global trend for stronger consumer data privacy laws will see bi-partisan support for this bill. Companies that have actively pursued compliance with the GDPR and CCPA will be in a prime position to become compliant with the CDPA through only minor updates/revisions to their internal and published policies.

Our experienced attorneys at Dickie, McCamey & Chilcote, P.C. have advised clients on international and domestic data privacy compliance for years and will continue to provide updates on this latest development (and others to be forthcoming of course) as the global trend toward stricter data privacy inevitably continues. If you have any questions or concerns, please contact us; and we will be happy to work with you and to help equip your company for compliance in this constantly evolving area.

The material on this site is for general informational purposes only and is not intended to be, and should not be construed to be, legal advice. There shall be no liability accepted as a result of any improper reliance on the material on this site. A qualified lawyer should always be consulted with regard to any specific legal issue or problem.