Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Will The US Match Or Improve On GDPR Privacy Model?

By **Jonathan Walsh and Edward Combs** (May 8, 2018, 12:50 PM EDT)

Jonathan Walsh

Edward Combs

Mark Zuckerberg's testimony before Congress on Facebook's role in the Cambridge Analytica data-sharing scandal has stoked a renewed interest in a regulatory solution to protect personal data and individual privacy in the U.S.

The European Union's response to similar pressures was to enact a comprehensive set of data privacy regulations in 2016 that will become effective May 25, 2018. With multiple — some might say competing — privacy solutions currently pending before Congress, it remains to be seen whether and how the U.S. will rise to meet this potential area of concern, and whether it will improve upon the regulatory model offered across the Atlantic.

The European Approach: The GDPR

The EU's General Data Protection Regulation is a comprehensive regulatory scheme for the personal data of EU residents.[1] It governs all European controllers or processors of personal data of data subjects who are in the EU, regardless of where the processing takes place. It also governs controllers and processors located outside the EU who process personal data of EU data subjects for a commercial purpose or track the behavior of EU data subjects.

These are the key features of the GDPR, which significantly change the regulatory landscape for data privacy and security, and could serve as a model for, or at least influence, any proposed U.S. legislation:

- The GDPR defines "personal data" broadly as any information relating to an identified or identifiable natural person. This includes "a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." The definition includes such data as internet protocol addresses, email addresses, and tracking data compiled through automated web traffic analytics.

- The GDPR requires that any entity processing personal data must have a lawful basis for doing so. Such bases include the data subject's free and unambiguous consent, necessity of the processing for the performance of a contract to which the data subject is a party, compliance

with a legal obligation to which the data controller is subject, and protection of the data subject's "vital interests."

- The GDPR mandates that each organization that controls or processes large quantities of personal information appoint a "data protection officer," who must oversee the organization's compliance with the GDPR's myriad requirements.

- The GDPR requires that regulated entities protect personal data by storing, processing, and using the data in a way that maintains the data subject's privacy "by design and by default."

- The GDPR contains provisions that allow data subjects to demand correction and erasure of their personal data, and limits the purposes for which the data controller or processor may hold or use the data.

- The GDPR obligates data controllers and processors to notify legal authorities "without undue delay" and in no case more than 72 hours after a data breach occurs.

- If a regulated organization violates any of these requirements, varying sanctions can be imposed, including a fine of €20 million or up to 4 percent of the annual worldwide turnover of the preceding financial year, whichever is greater.

The Opt-in Regime Approach: User Protection Through Consent — the BROWSER Act and the CONSENT Act

One bill proposed in Congress that signals a move towards GDPR-style data regulation here in the U.S. is the Balancing the Rights of Web Surfers Equally and Responsibly (BROWSER) Act, introduced by Rep. Marsha Blackburn, R-Tenn., last year.[2]

The BROWSER Act would impose new data usage requirements on internet service providers (such as AT&T and Verizon) and "edge service" providers (such as Facebook, Google and Twitter). The main provision of the BROWSER Act is the requirement that regulated entities obtain "opt-in approval" from users "to use, disclose, or permit access to" users' "sensitive information." This includes financial information, health information, geolocation information, the contents of any communication, any web browsing or software usage history, and any information pertaining to children under the age of 13.

"Opt-in approval" means that the covered services must obtain express consent for use of sensitive user information. This standard is more lenient than the similar provision under the GDPR, which specifies the way in which consent must be obtained and limits the effectiveness of that consent once given.

Requiring opt-in consent is, however, a significant change from the current opt-out regime in place in the U.S. that leaves many consumers unaware that they have surrendered certain privacy protections simply by continuing to use a service. The BROWSER Act would also prevent regulated entities from conditioning use of the service on waiver of data protection. In stark contrast to the GDPR, the BROWSER Act does not have significant exceptions for the use of data in connection with the performance of a contract or a legal obligation, potentially leaving service providers at the whim of their subscribers to consent to the use of their key personal data.

Congress is also considering the Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act,[3] which would place significant constraints on the "edge providers."

Notably, the bill would require the service providers to obtain explicit opt-in consent from users to use, share, or sell any personal information, as well as clear notification any time data is collected, shared, or used. Like the BROWSER Act, the CONSENT Act would prevent companies from conditioning uses of their services on a waiver of consent. For sensitive customer information that has been "de-identified," the CONSENT Act would implement protections to ensure that anonymous information stays anonymous. The CONSENT Act would also require that regulated internet services develop "reasonable data security practices," similar to the GDPR's "by design and by default" data security practices.

The Targeted Approach: Regulating Data Brokers — the DATA Act

Another proposed piece of legislation is the Data Broker Accountability and Transparency (DATA) Act,[4] which would regulate "data brokers" — companies whose core business is the collection and monetization of personal and sensitive information about consumers.

The bill would allow consumers to access and correct personal information held by data brokers such as Equifax. The proposed law would also bar data brokers from obtaining or causing to be disclosed personal information by making a false, fictitious, or fraudulent statement or representation; it would further consumers to request that data brokers stop using, sharing, or selling their personal information for marketing purposes.

The DATA Act would also require data brokers to develop privacy and data security programs, and provide notice to consumers in cases of data breaches. These provisions are similar to the portions of the GDPR that address data subject control of personal data and the right to be forgotten. The DATA Act, however, would be more limited in scope than the GDPR, as it focuses only on business entities that maintain information about individuals who are neither customers nor employees of the entity.

The Security Approach: Regulating Private Sector Companies – SPADA

The Secure and Protect Americans' Data Act[5] (SPADA) would mandate that the Federal Trade Commission introduce regulations detailing the new steps private-sector companies must take to avoid being hacked.

It would require regulated entities to continually review their data protection programs, ensure the accuracy of the private information they possess, and expeditiously notify consumers when their data was breached. The bill was reintroduced in 2017 after the infamous Equifax breach that affected hundreds of millions of Americans' credit data and puts new requirements on those who experience data breaches.

Imposing Criminal Penalties: Regulating Data Security and Breaches – the Data Security and Breach Notification Act

Lastly, one bill creates potential criminal penalties for data security breaches: the Data Security and Breach Notification Act.[6] Introduced by Sen. Bill Nelson, D-Fla., after Uber disclosed that hackers stole data on 57 million customers in 2016, the act would require companies to report data breaches within 30 days. Any person who intentionally and willfully conceals a data breach would be subject to up to five years in prison; this act would also provide for civil penalties against organizations that violate the law.

Some data breaches would be exempt from the legislation's requirements — for example, if only a last name, address or phone number is revealed, the law would not require disclosure. Mandatory

disclosure would also not apply if an organization "reasonably concludes that there is no reasonable risk of identity theft, fraud, or other unlawful conduct." The legislation would also direct the Federal Trade Commission to draft consumer-data security standards. Finally, the bill (like many of the other proposed solutions) would preempt the statutes and regulations of states that require similar information security practices and require disclosure of data security breaches. This is notable, as 48 states currently have data breach statutes in place, many of which could be nullified if this bill were to pass.

Conclusion

Each of these proposed legislative fixes stops well short of the comprehensive solution provided by the GDPR. While certain aspects of the proposed legislation mirror the European analogue, such as the requirement to obtain consent affirmatively in the BROWSER and CONSENT Acts and the basic requirements for data security in the CONSENT Act and SPADA, no proposed solution provides the level of government protection of user data (and corresponding bureaucratic control) engendered by the GDPR. By limiting the scope of the acts, however, lawmakers may create a narrower regulatory solution that is more palatable to U.S. businesses and consumers. Notably, these proposed legislative solutions do not provide for a private right of action against service providers or data brokers — a right that the EU saw fit to preserve and enhance in Chapter VIII of the GDPR. As a result, American consumers would have to rely on federal and state agencies to enforce their rights to privacy and pursue damages for data breaches.

The growing concerns over Facebook's use of customer information will most likely lead to more calls in Congress for a workable data protection regime, especially as the number of data breaches is expected to increase over the next few years. The United States' adoption of its own form of the GDPR has become a question of when, not if.

Jonathan Walsh is a partner and Edward Combs is an associate in the New York office of Curtis Mallet-Prevost Colt & Mosle LLP.

The authors thank Andrew Marino for his assistance preparing this article.

[1] Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016, General Data Protection Regulation, 2016 O.J. (L 119) 1-88.

[2] Balancing the Rights of Web Surfers Equally and Responsibly Act of 2017, H.R. 2520, 115th Cong. (2017).

[3] Customer Online Notification for Stopping Edge-provider Network Transgressions Act, S. 2639, 115th Cong. (2018).

[4] Data Broker Accountability and Transparency Act of 2017, S. 1815, 115th Cong. (2017).

[5] Secure and Protect Americans' Data Act, H.R. 3896, 115th Cong. (2017).

[6] Data Security and Breach Notification Act, S. 2179, 115th Cong. (2017).