GDPR in the U.S.: Be Careful What You Wish For

May 23, 2018

The current attention on the Facebook/Cambridge Analytica scandal has caused numerous commentators to suggest that the United States should adopt a law modeled after the European Union's General Data Protection Regulation (GDPR), which goes into effect on May 25, 2018. Indeed, even Facebook itself offered to provide its American users with the same protections provided for its European users. Interestingly, even as more and more Americans are citing GDPR as a model, very few seem to understand what GDPR actually demands. For example, in just the past couple of weeks I have heard GDPR summarized by a supposed expert as "a law that requires the consumer to opt-in to sharing their data;" a law that "establishes the right to be forgotten;" and "Europe's data breach notification law." Though there is truth in each of these claims, such summaries skip over so much about what GDPR mandates that it leaves people more, not less, confused as to what GDPR involves, and perhaps not coincidentally, allows companies to claim they are providing GDPR-like protections without really committing to very much.

Before explaining in more detail what GDPR compliance really entails, it is worth recounting the different approaches to data privacy that have developed in the U.S. and EU. The biggest major difference is that to date, outside of some heavily

regulated industries, such as health care and banking, the U.S. does not have generally applicable privacy regulations. Instead, decisions about what can be done with an individual's data are left to the company that holds that data, provided that the company has not been dishonest about how it intends to use the data (which would be a violation of various consumer protection statutes). This legal framework has resulted in very expansive terms of service written by companies that virtually all consumers click through without reading before signing onto a website. In this way, consumers in the U.S. have mostly chosen to provide data to companies with very few limitations in return for free or reduced cost access to the services the companies provide. These expansive terms of service are the first line of defense for any company alleged to have abused consumers' trust — essentially "you gave us permission" (even if you didn't realize you had done so).

The closest approximation the U.S. currently has to a broad-based data privacy regulation are the state data breach notification statutes. These statutes, which vary from state to state, generally require an organization to notify the affected individuals if it suffers a data breach that results in the loss of Personally Identifiable Information (PII), such as a Social Security number, credit card number, or date of birth. These are not really privacy statutes at all. Instead, they are entirely retroactive (they are implicated only after a security breach has occurred) and place no limits on what an organization can itself do with personal data provided that they keep it secure from unauthorized third parties.

The EU has taken a very different approach and not just in terms of the specific regulations it has applied. The EU has elevated data privacy into the realm of individual rights. Indeed, the very first paragraph of GDPR states, "The protection of natural persons in relation to the processing of personal data is a fundamental human right." GDPR then has an entire chapter devoted to the "rights of data subjects," which include the right to access data; the right to correct mistaken data; the right to move data to another platform or provider; the right to restrict or prohibit processing of data; and, most controversially, the right to erasure (sometimes called "the right to be forgotten"). These collection of rights, though not absolute even under European law, have no obvious analogue in U.S. law, and in some cases appear to conflict with our own legal rights. Thus, the "right to be forgotten" has been interpreted by the European Court of Justice to require Google, for example, to remove accurate but negative newspaper articles from search engine results because they were published long enough ago to no longer be deemed relevant. In the U.S., this would run squarely against Google's First Amendment free speech rights.

It may be that when people refer to "GDPR-like" protections, they are referring these data "rights," even if in the U.S. we might not choose to elevate the protections to the status of fundamental rights. The GDPR, however, includes far more. For example, another section of the GDPR only allows for the processing of personal data if it fits into one of only six legal bases. All other processing of personal data is thus deemed illegal. While one of the six bases is consent (hence the misleading claim that it is an

"opt-in" statute), Europe's definition of consent is far more restrictive than in the U.S. For example, it is difficult under European law to prove that an employee has given free consent if the consent is a job requirement. Thus, in some EU countries, there is considerable doubt whether consent to process data will always be a valid basis to allow data processing under GDPR.

Moreover, GDPR sets up an entire regulatory framework that goes far beyond these sorts of rights and responsibilities. It essentially mandates that companies hire a Data Protection Officer, regularly engage in Privacy Impact Assessments, include certain clauses in their contracts with third parties, partially restrict the transfer of personal data outside the EU, and provide both a government enforcement mechanism and a private right of action for those who believe they have had their data rights violated. GDPR (like U.S. data breach notification laws) also requires reporting in the case of a data breach, and provides a very short window (72 hours) for companies to make this report. And, most famously, the GDPR provides very steep fines for failure to comply — fines of the greater of €20,000,000 or 4 percent of global revenue. These fines dwarf the size of the largest settlements that have occurred in the U.S. for data breaches. Even without the fines, compliance with GDPR is complicated enough that it is expected to cost impacted companies millions of dollars.

Given all that, it seems unlikely the U.S. will adopt a privacy regulation as complicated and expensive as GDPR, and essentially inconceivable that a company such as Facebook would do so voluntarily. Instead, it is worth considering which aspects of GDPR are more compatible with U.S. law and tradition.

In my opinion, GDPR contains three sets of ideas that the U.S. would be wise to adopt:

First, companies ought to be required to replace (or at least augment) the impenetrable and unreadable terms of service agreements with a much more prominent and easy to understand description of how personal data will be used.

Second, organizations should be required to provide, upon request, certain information to consumers. For example, under EU law, a person can initiate a "subject access request" — essentially a demand to see all the information a company may have about that individual. Thus, if you want to know what Facebook is (or could be) telling advertisers about you, you could ask Facebook that question and they would be required to tell you. Facebook could also be required to provide your data in a way that allows you to transfer that data to a different social media platform. Similarly, in the EU, if you want to cancel your Facebook account, you can also request that Facebook remove whatever historical information it has about you from its database, and Facebook must either comply with that request or explain what legal basis it has for denying the request.

Third, the U.S. should create a single, national liability scheme for data privacy and data breaches, clarifying both the government's ability to fine companies for breaches and individuals' ability to sue if they are the victims of breaches. Replacing the current patchwork of state laws with a national law would not only benefit consumers, it would

make it far easier for companies who currently must navigate 50 different breach notification statutes.

The recent Facebook scandal shined a light on the shortcomings of U.S. privacy law, but we should be wary of claims that the answer lies in copying the European privacy framework.

Seth P. Berman leads Nutter's Privacy and Data Security practice group and is a partner in the firm's White Collar Defense practice group.

http://www.govtech.com/analysis/GDPR-in-the-US-Be-Careful-What-You-Wish-For.html