THE
NATIONAL LAW REVIEW

Why Startups Should Treat Data Privacy as a Cultural Issue

Thursday, May 16, 2019

Article By Varnum LLPStartup Blog
Jeffrey M. Stefan II

Corporate & Business Organizations
Administrative & Regulatory
All Federal

The times are definitely changing for any company that handles personal information and emerging companies need the right culture to address it. The U.S. has traditionally regulated data privacy through sector-specific laws, such as the Health Insurance Portability and Accountability Act but no comprehensive federal data privacy law or regulation exists. While every U.S. state has enacted some form of data privacy statute, variations exist among state law provisions. All of this provides flexibility for U.S. companies. The U.S. regulatory environment, however, could look very different in years to come. Prompted in part by a steady stream of highly publicized data mishaps, calls for more comprehensive data privacy regulation continue especially at the federal level. Moreover, California's Consumer Privacy Act of 2018 (CCPA) and the far-reaching EU General Data Protection Regulation (GDPR) are already impacting many U.S. companies. The laws' prescriptive frameworks could be modeled as an underlying basis for additional federal or state laws. This post briefly summarizes recent data privacy activity and stresses the need for emerging companies to build the right culture around data practices.

The CCPA and GDPR

Both the CCPA and GDPR prescribe very specific requirements for companies that handle personal data. While these laws are not identical, they both contain strict notice and consent requirements, mandate data portability and give consumers greater control over how their data is used by covered companies. The GDPR went into effect in May 2018 and the current compliance deadline for the CCPA is January 1, 2020. These laws have already caused many U.S. companies to reassess their data handling practices. And legislation has already been introduced in other states mimicking the CCPA's prescriptive regulatory approach for personal data. While both laws have been criticized, they could create a new norm for U.S. privacy expectations.

National Consumer Privacy Law?

The possibility also exists for comprehensive federal data privacy legislation as stakeholders become more concerned about privacy protections. Data privacy continues to be a talking point with 2020 presidential hopefuls Senator Klobuchar, in fact, referenced the need for privacy rules of the road during her campaign launch. On the other side of the aisle, Senator Marco Rubio introduced the American Data Dissemination Act (S. 142) that sets forth the framework for a national consumer data privacy law that would preempt state privacy laws, including the CCPA. This highlights a central challenge with passing a federal data privacy law, namely finding common ground on state preemption. State attorneys general oppose preemption on the grounds that they believe privacy enforcement should be handled under state law. On the other hand, many companies have advocated for a federal law that preempts the CCPA and other state privacy laws. These groups contend that the CCPA, in conjunction with the existing patchwork of state data privacy laws, creates unnecessary complexity and compliance difficulties.

There is no doubt that the debate over a comprehensive federal privacy law will continue. Though it is difficult to predict how these legislative efforts will play out, any company handling personal data needs to pay attention.

Culture and Key Questions

While keeping abreast of the latest data privacy law developments may not be top of mind for many emerging companies, it should not be ignored. Here are some baseline questions for emerging companies to assess their data privacy programs:

- Do you have clear internal guidelines as to how data will be collected, shared and disclosed? Are these materials easy to implement and understand? Do your company's practices reflect these guidelines? Do your employees take ownership of it? Do your company's leaders buy in?
- Do you communicate your data practices to your customers in a clear and concise manner? Do you have systems in place that would accommodate customer choice regarding their data? Note that both the CCPA and GDPR mandate data portability and this trend is likely to continue.
- Do you map and assess the quality of your data? Do you retain data that you do not need or use? Companies can alleviate some regulatory obligations by limiting their exposure to personal or sensitive consumer data that they do not need. You should ensure that any personal or sensitive data you collect is directly tied to the purposes for which you plan to use it and that you only collect it to the extent necessary for those purposes.
- Do you have practices in place to protect any personal or sensitive consumer information collected? Do these practices cover technical controls (e.g., anti-hacking software, firewalls), administrative controls (e.g., personnel restrictions, data classification) and physical controls (e.g., locks, swipe cards)? Do you need an independent evaluation? Have you have allocated appropriate resources for the issue?

The questions above will help, but ultimately the best way to deal with data privacy from both a legal and customer-centric standpoint is to develop cultural values centered around sound data practices. To borrow a term from Beth Hill's recent and persuasive writing, *Privacy, Culture and Data Respect* [1], the culture should be one that respects data. As she explains:

If a core principle of an entity is 'we will treat all data with respect,' then all behavior related to that data will flow from that principle. For example, consider the following questions:

Will you encrypt the data when sending to a third party even though it requires two extra steps? Yes.

Will you be sure that you have the appropriate permission to use the data in the way you want to, even if no one will ever find out that you don't know if you have that permission? Yes....

Culture, whether it eats strategy for breakfast or not, is important and should never be underestimated....Culture is a living thing that grows from within; a series of some large decisions that result in many small decisions that beget thousands of decisions made every day within an organization. Creating a culture of respect for data will have a positive net effect within organizations that subscribe to it.

Policies and procedures have no life without underlying culture. The best-written policies or the clearest legal advice is useless if they do not facilitate consistent action through all facets of the organization. Emerging companies that do not treat data as a cultural issue do so at their own risk in today's environment.

[1] Beth Hill is Ford Direct's General Counsel and Chief Compliance Officer. Her article can be found at https://www.linkedin.com/pulse/privacy-culture-data-respect-beth-hill/

Source URL: https://www.natlawreview.com/article/why-startups-should-treat-data-privacy-cultural-issue