HINSHAW

How Ancient Wisdom Can Illuminate Data Privacy Compliance for Both Newcomers And Hold-Outs

Hinshaw Alert | 6 min read
Aug 23, 2022

Augustus Caesar once said, “if you want a rainbow, you have to deal with the rain.” Presumably, this was said—in Latin—after he overhauled all aspects of ancient Roman life. Thousands of years later, the same sentiment holds true for those struggling with the quagmire of data privacy and protection laws proliferating in the United States (U.S.) and seeking to understand what they can do with the data they have collected in light of those laws. While compliance and understanding may feel like a colossal chore, in the end, you and your business might find that it was well worth the effort.

Before we dive into the law, we should first discuss why this space is being regulated. After all, judging by what consumers post online, it would seem that they are only too happy to part with personal and sensitive information. While that may be true, it is unlikely that most consumers know just how much information about them is being collected. Everyone is familiar with or has heard of “cookies,”—the files a website places on a device to track a user across the internet. However, most people don’t know that even if they have the option of opting out of such tracking, there are still alternative means of identifying them and their interests online.

Device fingerprinting is one such alternative. This technique involves identifying an electronic device based on its unique configurations. This method of identification tracks signals such as a user’s IP address, the resolution of their computer screen, the size of their browser, and even how they move their mouse. Traditionally used for security purposes, it is now being used by marketers to connect online identities to real-world ones. Because it does not require local storage on a user’s device, such fingerprinting is very difficult to circumvent and has become known as the “cookie-less monster.”

Another identification tool in use involves the metadata associated with text, voice, and email messages. Even if the content of the message is encrypted, other information—such as the identity of the sender and recipient, the time of day it was sent, and how often the communication occurred—is still very revealing. For example, if you call a cardiologist, it could be inferred that you or someone you know has a heart problem. Expect to see advertisements for everything from Cheerios to baby aspirin the next time you go online. You might also

experience a strong case of what has been coined “algorithmic anxiety,”—the unease associated with contending with machine-based estimations of one’s needs and desires.

Beyond being unsettling, there is also the potential for abuse and discrimination when data is collected and used in a behind-the-scenes manner. Nevertheless, companies can generally still collect, share, and sell all types of data in most states without providing any notice to consumers. This is due in large part to the fact that the United States does not have a singular data privacy law at the federal level. Instead, the United States has a mix of laws that regulate certain sectors and types of sensitive information. If acronyms like HIPPA, FCRA, ECPA, and GLBA sound familiar, then you likely already have at least some understanding of this approach, and possibly its shortcomings.

The absence of a federal privacy law left a vacuum that states like California, Connecticut, Colorado, Utah, and Virginia attempted to fill. For example, the California Consumer Privacy Act (CCPA)—the most comprehensive state law that is focused on in this article—and the amendments expanding on the CCPA, the California Privacy Rights Act (CPRA), require that businesses inform consumers regarding the types of personal data they collect at the time they collect it and also how the information will be used. In other words—and this true of most if not all data privacy laws—the key is transparency.

Significantly, unlike other laws, the CCPA does not require that a company obtain consent before collecting or using personal information. Consent generally only becomes an issue if a company shares personal information for a commercial purpose, *i.e.*, sells the information. The term “sale” is broadly defined under the CCPA and covers any situation where information is shared with a third party in exchange for something of value, financial or otherwise. A business is not selling personal information under the CCPA if the consumer consents to sharing it or the data is used for a reasonable business purpose. Generally, if data is used in a way that is consistent with how a consumer might expect it to be used, then it likely falls into the business purpose category.

Covered entities also have obligations when it comes to sensitive information, which includes social security numbers, driver’s license numbers, passport numbers, financial account, and payment card information, precise geolocation, and health and biometric information. It also includes categories like ethnicity, religion, and sexual orientation. In addition to disclosing the types of sensitive personal information they collect and the purposes for collection, businesses must provide a clear and conspicuous link on their website homepage, entitled “Limit the Use of My Sensitive Personal Information,” that enables a consumer to limit the use or disclosure of the consumer’s sensitive information.

Suppose your business wants to use the data it has collected to draw inferences about a consumer. At least in California, those inferences are considered personal information and must be disclosed to the consumer if they make a right-to-know request—one of the many rights Californians currently enjoy under the CCPA. How long they will enjoy all of those rights is currently a matter of public concern and debate. In July of this year, with bipartisan support, a proposed federal data privacy and protection law, the American Data Privacy and Protection Act (ADPPA), containing a controversial pre-emption provision, was sent to the House for a vote—the furthest any such proposed federal law has ever gone.

What would enactment of the ADPPA mean for your business? For starters, it would mean that the patchwork of state privacy laws would essentially be whittled down to one federal law. While the ADPPA also requires consent in certain situations, it focuses more on data minimization, which means collecting and retaining for a reasonable amount of time only the data you need to accomplish a specific task. Even if the ADPPA never becomes law, data minimization is still a good security practice and, in any event, a requirement under the CPRA.

In the meantime, in addition to state laws, businesses must also be mindful that various government agencies such as the Consumer Financial Protection Bureau (CFPB), the Securities and Exchange Commission (SEC), and the Federal Trade Commission (FTC) are all using their powers to police this space. For example, on August 11th of this year, the CFPB published a circular finding that insufficient data protection or information security violates the prohibition on unfair acts or practices. Similarly, the SEC recently collected $2.1 million in combined penalties from two U.S. brokerages for allegedly failing to have proper policies and procedures in place to detect identity theft. Not to be outdone, the FTC recently threatened to sue an ad tech company it alleges reveals people's sensitive locations, which it claims violates laws that prohibit unfair and deceptive practices. Notably, these are only recent examples of agency enforcement.

As you have likely surmised, the current regulatory environment is multi-layered and rapidly evolving. To avoid legal issues, it is essential that you and your business adapt. Even if you think your business is well positioned, you need to stop and ask, if a regulator showed up tomorrow, would I be comfortable with what they found? If you did not answer that question in the affirmative within seconds, went pale, gulped, or had to think, then it's probably safe to say that you and your business have work to do.

Aside from avoiding legal woes, there is another reason why compliance is important. More and more consumers are starting to expect it because this topic has gone viral in a global way. Consequently, many companies, whether they be national or international, are starting to weave privacy into all the many facets of their business and advertising their efforts to good effect. In other words, once you get through the rain and get your business organized and in compliance, there could be a big pot of gold at the end of that proverbial rainbow.

Related People

Jason J. Oliveri

Partner

212-471-6237

Related Capabilities

Data Privacy, AI & Cybersecurity