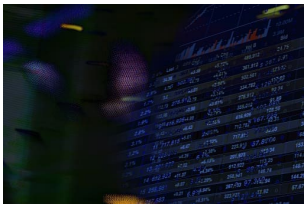

Cashing in on Personal Data? Not So Fast!

Jun 02, 2021

Categories:

Publications
Technology Blog

Authors:

Michael E. Nitardy

Industry analysts and business consultants have agreed for some time that connected mobility is the wave of the future. Most companies are coming to the realization that data is, and will be, the fuel that drives the connected mobility industry. The provision of a single, connected vehicle platform across multiple different services represents an attractive option for companies exploring ways to monetize data. But companies may be tempted to adopt the technology necessary to be successful with their data monetization efforts while neglecting the worldwide data protection laws and regulations that must be followed. The adoption of a data monetization strategy without the corresponding adoption of a data privacy and security compliance program may result in financial losses, not gains.

Below, we explore three reasons why a data privacy and security compliance program should be a part of any company's adoption of a data monetization strategy.

Compliance is required.

Advances in technology will undoubtedly help record, collect, store, and analyze vast amounts of data that the customer never realized was possible. Data points that were once deemed to not be personal information, and thus not subject to data protection laws, are now considered personal information under both the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Under GDPR Article 4 (1), "personal data" "means ***any information relating to an identified or identifiable natural person*** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as 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." (Emphasis added).

Cal. Civ. Code § 1798.140 defines "personal information" as "information that identifies, relates to, describes, ***is reasonably capable of being associated with, or could reasonably be linked***, directly or indirectly, with a particular consumer or household." (Emphasis added).

But the GDPR and CCPA are not the only data protection regimes to be concerned about. Brazil recently implemented its new privacy legislation, the General Personal Data Protection Act (LGPD). Additionally, in the past several months, China released its draft privacy legislation, California passed legislation strengthening the CCPA, and both Canada and India have announced they will consider new data protection regimes. In the U.S., there are several proposals pending for a uniform federal privacy law.

Though no two regulatory regimes are identical, they all share overarching themes that can be used to implement a standard compliance program. For instance, all regulatory regimes include the concepts of providing consumers notice, a requirement of consumers' consent or other legal basis for use of the information, a right to access and correct their information, and a right to object to the use of their information. A compliance program will help companies navigate these laws and regulations. The first critical step is to identify the specific types of data to be collected, processed, and secured. Next, the company should identify the specific in-scope data protection laws and regulations applicable to that data. After determining this information, the organization can craft a compliance strategy that works with the available technology to account for and secure all applicable data.

Compliance is expected.

Consumer surveys and market studies all confirm what we intuitively know: Consumers are more trusting with their data with organizations that are transparent about their data practices. Developing a compliance program is a prerequisite to transparency. Unfortunately, many businesses initially choose what they perceive to be the least onerous compliance strategy (i.e., failing to adopt one), while hoping to pivot to compliance if forced to by legal necessity. While having some initial benefits (speed, simplicity, etc.),

this tactic may work against the organization's goal for tech intensity and could cost the company many times more than it intended to save.

If data is the fuel of the new connected mobility, the supply and quality of the fuel is very important. The major data protection laws include avenues for consumers to object to the use of their data, request deletion of their data, and withdraw consent for the use of the data. Such rights make it imperative that companies do everything they can to foster consumer confidence. Accordingly, a compliance program that has identified the data collected by the organization and the laws applicable to the data is just the start. Last year, the European Data Protection Board (EDPB) issued "Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications," with general recommendations for vehicle and equipment manufactures to mitigate the risks of violating privacy rights when personal data is processed by connected vehicles. The EDPB made the following recommendations:

- Geolocation data, biometric data and any data which could reveal a criminal offense should be given special attention.
- Technologies should be designed to minimize the collection of personal data.
- Local data processing should be used as much as possible to minimize the potential for transferring personal data outside of the vehicle.
- Anonymization and pseudonymization should be used where data is being transferred outside of the vehicle.
- Tools should provide functionalities that enable individuals to exercise their right to control their data during the entire processing period.
- All traditional methods of increasing security and confidentiality should be used (e.g., encryption and key management).
- The technology should make it easy to both give consent and take it away.

Non-compliance is expensive.

Frost Brown Todd's Privacy and Data Security Team provides a weekly update of the top privacy and security stories from around the world. Inevitably, each week includes a story about another fine levied by a regulatory authority or a settlement reached with either an attorney general or a plaintiff's attorney. A company's failure to comply with privacy and security laws is expensive. The average cost of a breach in 2020 was estimated to be over $3.8 million. European regulators issued over €175 million in fines in 2020.

A data breach can prove fatal to a company's bottom line. Expenses to recover systems, contain damages after a breach or regulatory action, or to pay fines are just the beginning. Companies also stand to suffer significant reputational damage with resulting downturns in the company's market share, revenue, and social capital over the short and long term. While some companies can absorb these costs, they could bankrupt others.

Companies must be aware that plaintiffs' lawyers and diligent governmental regulators are on the prowl. To stave off the costs associated with a breach or regulatory action, a good compliance program should focus on both privacy compliance *and* data security. They are two sides of the same coin, and one should not be neglected for the other. Companies that invest early and often in compliance stand to mitigate risks while positioning themselves for outsized returns on their data monetization strategies.

Questions? Contact Mike Nitardy of Frost Brown Todd's Privacy & Data Security and Mobility & Transportation teams.

Associated Industries and Practices: Mobility & Transportation | Automotive | Technology | Privacy & Data Security | Intellectual Property

FBT Gibbons