The Need for Balance: Exploring Law and Policy Regarding the Protection of Personal Data

Brett Cook, JD, LLM
Associate General Counsel,
Data Privacy/Regulatory Compliance
Fort Worth, Texas
Email: Brett.d.cook@gmail.com

Author Note

This article will explore the need to balance the desire to collect and process personal data with the need to preserve privacy. Emerging European Union (EU) and United States (US) state laws will significantly impact the collection and processing of personal data by global corporations. The inherent tension between the need to collect personal data and maintain privacy protection shapes how we perceive businesses who rely on this information to increase profits and advance humanity.

The author is solely responsible for the contents of this article. The contents do not necessarily reflect the position of any of the institutions the author serves. The author has no financial conflicts of interest.

Introduction

In his book *Zero to One: Notes on Startups, or How to Build the Future*, Peter Thiel explains that the next world-changing company will discover something that is important to people and difficult to achieve. For example, *Air BnB* discovered the need for affordable lodging and an untapped resource: property owners who desire to easily and reliably rent their unoccupied space. Likewise, *Uber* and *Lyft* discovered a way to connect people who need fast, reliable transportation with people who can meet this need without maneuvering through the bureaucracy of a heavily-regulated taxi industry.

Today, another need has emerged: the need for a secure and transparent data collection process. Companies are searching for avenues to combine their desire for large amounts of personal data with a process to safely collect, retain and transfer this information. Previously, a lack of federal and state regulations allowed companies to utilize self-regulating data privacy policies to assure consumers that their information was being responsibly handled. These policies continue to add value by providing a comprehensive explanation of how and why personal data is collected, which produces competition to create policies that resonate with customers. Nonetheless, recent EU and state laws governing personal data collection demonstrate that consumers are reluctant to allow capitalism and innovation to drive this process.

GDPR: The EU's Comprehensive Data Privacy Law

Last May, the EU implemented the General Data Protection Regulation (GDPR), a law that provided explicit data protection and privacy for all individuals within the EU and the European

Economic Area (EEA). The GDPR also regulates the export of personal data outside EU and EEA areas. In summary, if you are an EU company or a company that processes EU citizens' personal data, you are now subject to heavy fines if you are not compliant with the GDPR.

Definition of Personal Data and Processing

The impact of the GDPR is significant because of its broad definition of "personal data" and "processing." The GDPR defines personal data as any information relating to an identified or identifiable person (aka data subject). An identifiable natural person is one who can be identified in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier. This also includes people who can be identified by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social information.

Processing personal data is defined as any operation or set of operations which are performed using personal data or on sets of personal data, such as collecting, recording, organizing, structuring, storage or adaptation. Alteration, retrieval, consultation, use, dissemination or otherwise making the data available is also considered data processing. Under the GDPR, EU citizens have the following rights:

(1) to request a copy of the data that was collected;

(2) demand that their data be deleted;

(3) be notified when their data has been hacked;

(4) provided an opportunity to consent to the collection of their personal data; and

(5) data protection safeguards, which must be built into products and services from the earliest stage of development.

Additionally, the GDPR prohibits forced consent and any form of service bundling in order to require consent. Consequently, access to services can no longer depend on whether a user gives consent to the use of data. The GDPR had an immediate impact in the US. Google, Instagram, WhatsApp, and Facebook were sued when the GDPR was enacted in May 2018 due to "forced consent" practices which required users to consent to personal data collection in order to use their products.

Expansive Territorial Scope

The increased territorial scope of the GDPR is a significant change to the regulatory landscape of data privacy, as it applies to all companies processing personal data of people residing in the Union, regardless of the company's location. Thus, GDPR applies to the processing of EU citizens' data, collection activities that relate to offering goods or services to EU citizens and behavior monitoring that takes place within the EU. Non-EU businesses processing this data also have to appoint a representative in the EU.

The GDPR has impacted US Fortune 500 companies who rely on online data collection to create and improve their products. In May 2018, Forbes reported that the GDPR has cost US-based companies nearly $7.8 billion in compliance activities to avoid potentially multi-million-dollar fines and penalties.

Corporate Governance Programs are Now Required

The GDPR places onerous accountability obligations on controllers and processors to demonstrate compliance with the law. Some of the elements that must be demonstrated are explicit. However, some are implied, such as the implementation of appropriate governance models so that data protection receives an appropriate level of attention within the organization. As a result, large organizations will need to implement formal data protection programs that include training, audits and C-level oversight. These requirements are relatively new to the US private sector. The GDPR has created a forcing function to ensure corporate oversight. On the other hand, US federal agencies, such as the Department of Defense (DoD) mandate that departments maintain robust data privacy oversight programs. This form of directed accountability is one of several areas where US public agencies have been ahead of private corporations regarding personal data protection.

US Data Privacy Laws

The California Consumer Privacy Act of 2018

On June 28, 2018, California lawmakers enacted the California Consumer Privacy Act of 2018 (CCPA). This is a sweeping privacy law, similar to the GDPR, with comparable reach and implications. The law takes effect on January 1, 2020, and will be enforceable in California and applies to California consumers. The CCPA is the first US state law to incorporate certain provisions already enacted in Europe under GDPR. However, companies that restructured their operations to comply with GDPR will have to expand their efforts under the CCPA. As discussed below, other states have followed suit, requiring businesses to trace and track the source of their data.

CCPA's Definition of Personal Information

The CCPA defines "personal information" (PI) as any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked with a particular consumer or household. Specifically, PI includes:

(1) identifiers such as any unique personal identifier or IP address;

(2) electronic network activity information, including, browser histories, search history, and any information regarding a consumer's interaction with a website, application or advertisement;

(3) audio, electronic, visual, thermal, and olfactory information; and

(4) geolocation data.

In addition, the Act specifies that any "inferences drawn" from various data elements of PI to create a profile about a consumer reflecting the consumer's preference, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities and aptitudes constitute PI. The CCPA's inclusion of PI data elements used to create consumer profiles directly impacts Bay Area tech companies who rely on this data to measure consumer preferences, behaviors, tendencies, etc. to predict market trends and focus advertising.

Under the CCPA, consumers will have a right to the following actions:

(1) request that a business disclose the categories and specific pieces of personal information that it collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of 3rd parties with which the information is shared;

(2) request deletion of personal information and would require the business to delete upon receipt of a request;

(3) request that a business that sells the consumer's personal information, or discloses it for a business purpose, disclose the categories of information that it collects and categories of information and the identity of 3rd parties to which the information was sold or disclosed; and

(4) to opt out of the sale of personal information by a business.

Businesses are prohibited from discriminating against the consumer for exercising these rights, by charging the consumer who opts out a different price or providing the consumer a different quality of goods or services.

Covered Entities

The CCPA applies to businesses that collect information from California residents and meet at least one of the following thresholds:

(1) have over $25 million in annual gross revenue;

(2) buy, receive, sell, or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or

(3) derive 50 percent or more of their revenue from the sale of consumers' personal information.

Additional States With Similar Data Privacy Laws

Several other US states have introduced and passed legislation that mirrors the protections provided by Europe's GDPR and expands data breach notification rules. These state laws are intended to provide consumers with greater transparency and control over their personal data. For example, California and Vermont's data privacy laws go beyond breach notification and require companies to make significant changes in their data processing operations.

The following are some important notations regarding these state laws.

- Alabama, Arizona, Colorado, Louisiana, Oregon, South Carolina, South Dakota and Virginia have passed laws defining personal data and specifying data breach notification requirements.
- Vermont's data privacy law regulates data brokers who collect and sell consumer data to 3rd parties.
- Commercial entities that conduct business in Nebraska and license, own or maintain computerized data that includes Nebraska resident's personal information must

implement and maintain reasonable security procedures and practices. In addition, commercial entities must contractually require non-affiliated, 3rd party service providers to institute and maintain reasonable security procedures and practices.

- Under Colorado's data protection law, organizations who maintain, own or license personal identifying information in the course of their business are accountable for protecting personal information. Similar to the GDPR, Colorado requires covered entities to: (1) develop and maintain written policies on the disposal of personal information; and, (2) implement reasonable security procedures and practices commensurate with the sensitivity of the processed data and the size and complexity of the company.
- Iowa's law includes companies that operate internet sites, online services, online applications, or mobile applications that are used primarily for K-12 students. It requires operators to implement and maintain security procedures and practices appropriate and consistent with industry standards and applicable state and federal laws, rules, and regulations.

At least 24 states have laws that address data security practices for private sector entities. Most of these laws require businesses that own, license, or maintain personal information about a resident of that state to implement and maintain reasonable security procedures and practices appropriate to the nature of the information and to protect personal information from unauthorized access or disclosure. Given the global nature of data processing, companies will need to determine when to apply the GDPR versus state data privacy laws to maximize their effectiveness.

Tech Industry Personal Data Collection Policies

Facebook

Facebook is a well-known social media company that relies on data collection. Facebook collects the content, communications and other information consumers provide when they use its products, including when they sign up for an account, create or share content, and message or communicate with others. Facebook also collects user metadata, such as the location of a photo or the date a file was created. The company utilizes this data to improve its products; provide analytics and business services; and promote safety and security. Facebook also uses this information to conduct research and innovation in support of general social welfare and public interest groups. The collected data can also include what consumers see through features Facebook provides, such as their camera, so they can suggest masks and filters that users might like or give tips on using camera formats. Further, Facebook employs data privacy policies that govern the collection and use of consumer data by Facebook and 3rd party developers who use their platform.

In some ways, Facebook's policies extend beyond GDPR and US state law. Their policies forbid developers from using data collected on their platforms to make hiring decisions or sell or license data obtained through Facebook. Additionally, data obtained from Facebook cannot be used to make decisions regarding financial eligibility, including whether to approve or reject a loan application or how much interest should be charged.

Apple

Similar to Facebook, Apple also uses personal information to create, develop, operate, deliver, and improve its products, services, content and advertising. Apple uses personal information for internal purposes such as auditing, data analysis, and loss prevention and anti-fraud purposes. They collect a variety of information, including names, mailing addresses, phone numbers, email addresses, device identifiers, IP addresses, and location information. Apple also collects credit card information when users create an Apple ID, apply for commercial credit or purchase a product.

Apple has cracked down on apps that do not communicate to users how their personal data is used, secured or shared. As of October 3, 2018, Apple requires that all apps have a privacy policy. Though the app makers themselves would be ultimately responsible for their customers' data, Apple, as the platform where those apps are hosted, is acknowledging that it has some responsibility too. All apps must include a link to their privacy policy and it must clearly identify what data the app collects, how the data is used and how a user can revoke consent or request deletion of their data. The policy must also confirm that any third party with whom the app shares user data will provide the same protection of user data as stated in the app's privacy policy.

Who is Accountable for Data Privacy?

Major tech company platforms are being held accountable for the behavior of 3rd party app developers and any data misuse that occurs as a result of their policies governing those apps. The extension of a company's data privacy policy to 3rd party developers is not surprising. These developers use the data, services and tools obtained through platforms like Facebook and Apple's Operating System (OS) to enhance their products and expand their impact. Facebook CEO Mark Zuckerberg, for example, was required to appear before the US Senate about the Cambridge Analytica incident, where data from 87 million Facebook users were inappropriately obtained and used by a 3rd party developer. In response to app developer misuse incidents like Cambridge Analytica, companies like Facebook and Apple have added muscle to their data privacy policies. Today, these tech giants, and others like them, employ independent policy enforcement and investigation divisions dedicated to identifying apps who violate their policies and preventing future misuse.

Conclusion

As it is known today, "big data" processing has shaped the way companies expand impact and increase profits. Successful tech companies, like those who provide social and professional networking platforms, are fueled by millions of apps and tremendous amounts of personal data. If processed correctly, this data can reveal precious, hidden information and lead to ground-breaking discoveries. Nevertheless, there is a need for balance and wisdom. Data can help advance who we are and what we can develop, but we must respect the personhood of those whose data provide acts of learning and innovation. In 2018, privacy commissions and industry regulators moved their chess pieces into place. The message: Privacy and data responsibility must be as important to the officers of a business as profitability is to the investors.

References

Apple Privacy Policy. (2019, February 18). Retrieved from https://www.apple.com/legal/privacy/en-ww/.

Facebook Data Policy. (2019, February 18). Retrieved from https://www.facebook.com/policy.php#.

Facebook for Developers. (2019, February 18). Retrieved from https://developers.facebook.com/policy/.

GDPR Key Changes. (2019, February). *EU GDPR.Org*. Retrieved from https://eugdpr.org/the-regulation/.

GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook. (2018, May). *European Center for Digital Rights*. Retrieved from https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf.

National Conference of State Legislatures, (2019, January). Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

Perez, S. (2018). Apple will Require all Apps to Have a Privacy Policy as of October 3. *Tech Crunch*. Retrieved from https://techcrunch.com/2018/08/31/apple-will-require-all-apps-to-have-a-privacy-policy-as-of-october-3/.

Persson, S., Serrato, J.K., Fernandez, A., & Rudawksi, A. (2018, June 29). California passes major legislation, expanding consumer privacy rights and legal exposure for US and global companies. *Data Protection Report*. Retrieved from https://www.dataprotectionreport.com/2018/06/california-passes-major-privacy-legislation-expanding-consumer-privacy-rights/.

Regulation (EU) 2016/679. *Official Journal of the European Union*, Vol. L119 (4 May 2016), pp. 1-88.

Serrato, J.K., Cwalina, C., Rudawski, A. (2018, July 9). US states pass data protection laws on the heels of the GDP. *Data Protection Report*. Retrieved from https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/.

Smith, O. (2018, May 2). The GDPR Racket: Who's Making Money From This $9 bn Business Shakedown. *Forbes*. Retrieved from: https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#336a48db34a2.

The California Consumer Protection Act. California Assembly Bill No. 375.

Thiel, P. (2014). *Zero to One: Notes on Startups, or How to Build the Future*. New York: Crown Publishing Group.