David J. Kim
CYBR 623
11/21/2021

Paper #2 - General Data Protection Regulation

In today's competitive business environment, the most successful corporations in the United States have depended on intensive analytics of their users' digital behavior in order to build, maintain, and increase their market cap. In the past, legal scholars and government officials genuinely believed nascent tech corporations would exhibit the precocious maturity and extraordinary restraint required in order to implement data privacy protections on their own without government intervention. However, public scandals such as Facebook's voluntary involvement with Cambridge Analytica clearly reveal that corporations have enormous financial incentives to gather, store, and sell the personally identifiable information of their end users. Historically, it has been legal for a business to process the personal data of end users and subsequently mine that data for a purpose that is different than the original context. In response, European lawmakers passed and codified the General Data Protection Regulation (GDPR) on May 25th 2018.

In this paper, I first examine in detail the various elements of GDPR and explain how its principles might be applied across various technical implementations. Next, I identify what consumer data protections currently exist in the United States at the federal level, and provide historical context regarding why our data privacy laws are different. Third, I explain the potential impact of GDPR on American companies, most notably a massive fine for valid data privacy violations "up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total world annual turnover of the preceding financial year, whichever is higher." (GDPR, Article 83, n.d.) Finally, I evaluate what the impact of GDPR has been in the past 3 years since its debut, and discuss what future changes to data privacy laws should be enacted to ensure future accountability.

According to Article 5 of the GDPR, six specific guidelines have been laid out to serve as philosophical principles that collectively constitute data privacy. Those principles

are 1.) fairness and lawfulness; 2.) purpose limitation; 3.) data minimization; 4.) accuracy; 5.) storage limitation; and 6.) integrity and confidentiality. (Goddard, 2017) Many of these data security principles will already be familiar to experienced cybersecurity professionals, however the explicit identification of these different principles in a single written document is clarificatory. In addition to these guidelines, GDPR also stipulates, guarantees, and enshrines certain functionalities to be accessible on the part of end users. These functional rights include the “right to erasure”, “right to access”, “right to rectification”, “right to data portability”, and also “right to restriction of processing.” (Bozhanov, 2018) This means that any business wishing to provide digital services to EU citizens covered by GDPR, must also figure out a way to implement these user-requestable functionalities.

The exact method regarding how different organizations will choose to implement each of these GDPR requirements will be incumbent upon each individual organization and their technical engineering team to settle upon and then execute. Different programming languages, paradigms, and toolkits will be more or less suitable according to the particular use case and functional right a business is attempting to build out. For example, perhaps an EU business owner wants to implement the “right of erasure” into his database that contains the home address shipping information of his customers. Doing so would also fulfill the Article 5 GDPR guidelines of 3.) data minimization and even more directly 5.) storage limitation. A hypothetical means of implementing this functionality into programming code might entail establishing a database column for data retention and deletion deadlines. The database could then query the tracking information of a particular customer’s shipment, and then automatically schedule for job deletion that customer’s personal home address information once the API for shipment tracking returns a true boolean value. (Bozhanov, 2018) Best practices for “pseudonymization” of personal data, perhaps via the use of an encryption key or obfuscation algorithm, should also be included within organizational policies that better ensure non-attribution of personal data. (Politou, 2017)

Next, specific instructions have been laid out by GDPR that address the methods and authoritative means by which informed consent can be provided by end users, prior to

collecting their personal data. According to the Court of Justice of the EU, in order for consent to be freely given and informed, it must be a “separate action” from the activity the user was initially pursuing. (Nouwens, 2020) In other words, this means merely visiting an online application and browsing it does not constitute a meaningful positive action and therefore does not provide informed consent. Instead, a user must provide explicit “opt-in” consent and a check-box must not automatically be filled in by default. (Nouwens, 2020)

Now that a technical discussion regarding the scope and general requirements of GDPR has been established, I move next to discuss part 2 of this paper regarding what consumer data protections currently exist in the United States. In comparison to Europe, the United States has a very different outlook on individual data privacy. Unlike data protection laws found in Europe, those laws in the United States have been siloed into specific categories corresponding to the particular business industry to which that data belongs.

> The categories covered under federal law are healthcare data (under the Health Information and Portability Accountability Act, HIPAA), financial data (under the Gramm Leach Bliley Act, GLB) children’s information (under the Children’s Online Privacy Protection Act, COPPA), students’ personal information (under Family Educational Rights and Privacy Act, FERPA), and consumer information (under the Fair Credit Reporting Act, FCRA) (Houser, Voss, 2018)

It is illustrative to notice two points. First, many of these statutes were enacted prior to the proliferation of the internet and correspondingly do not map very intuitively to the current digital landscape in 2021. Second, many of these laws approach data protection from the perspective of the business rather than the consumer. While the EU seems to frame data protection in the GDPR from the fiduciary perspective of individuals, the United States has heretofore been more concerned with enshrining the legal rights of mega-cap corporations. This includes continued protection of corporations’ legal authority to mine and sell the personal data of individuals. These vast differences in privacy rights ideologies can be traced back to the expressed inclusion of a “right to privacy” in the Charter of Fundamental Rights of the European Union, whereas no such equivalent legal guarantee exists in the United States Constitution. (Houser, Voss, 2018)

In the 3rd part of my paper, I now move to illustrate the concrete effects the passage of GDPR is likely to have upon American businesses. In a globalized economy and increasingly digital marketplace, it is difficult to avoid doing business with consumers located in various countries located across the world including the European Union. Despite this, there are many new business challenges that GDPR introduces to an already strained economic environment. Those include extraterritorial application of GDPR fines to data processors located outside the EU, specific functional rights granted to individual users (as previously discussed in this paper), and a host of new compliance mechanisms and audit-proof record-keeping requirements. (Rahman, 2018)

According to Article 83 of the GDPR, corporations found liable for violating the most serious category of data protection laws will be fined the higher of 20,000,000 EUR or 4% of their global annual revenue. This would entail a fine of $1 billion USD in the case of Facebook, or $3-4 billion USD in the case of Google/Alphabet. Such exorbitant fines represent a potential existential threat for Google's future ability to operate in the European marketplace precisely because a significant portion of their revenue stems from selling targeted advertisements using the data collected from European users. In 2014, the Italian Data Processing Authority (DPA) ordered Google to provide "more effective notices" and "obtain prior consent from its users for the processing of their personal information." Upon further technical investigation, it was discovered that Google was processing information in Gmail accounts and using data processing on cookies to profile users and sell targeted ads. (Houser, Voss, 2018) It remains to be seen whether Google and Facebook will successfully be able to adapt their data processing systems in order to maintain compliance with the European marketplace, or whether GDPR truly represents an existential threat to the future operations of their business model.

Since the introduction of legal enforcement of GDPR on the 25th of May 2018, the impact GDPR has had on the worldwide digital economy and the field of cybersecurity law has been immense and will continue to have drastic implications for the future of digital privacy. Certainly, the maximum fine that can be imposed under GDPR is unprecedented,

but perhaps the more importantly, the passage of GDPR has raised global collective awareness that the services mega-cap tech giants provide are not free. End users in the United States and abroad have started to understand that they themselves are the commodity these corporations are selling, at the significant expense of their personal data privacy.

References (APA)

Bozhanov, B. (2018, February 19). *GDPR - A practical guide for developers and architects*. AxonIQ. Retrieved November 22, 2021, from https://lp.axoniq.io/gdpr-data-protection-module.

GDPR Resources and Information. (n.d.). *Article 5: Principles relating to processing of personal data*. GDPR.org. Retrieved November 21, 2021, from https://www.gdpr.org/regulation/article-5.html.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. International Journal of Market Research, 59(6), 703–705. https://doi.org/10.2501/IJMR-2017-050

Houser, K., & Voss, G. (2018, November 6). *GDPR: The end of google and Facebook or a new paradigm in data privacy?* Richmond Journal of Law and Technology. Retrieved November 21, 2021, from https://jolt.richmond.edu/gdpr-the-end-of-google-and-facebook-or-a-new-paradigm-in-data-privacy/.

Nouwens, M., Liccardi, I., & Veale, M. (2020, April 1). *Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence*. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence | Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Retrieved November 21, 2021, from https://dl.acm.org/doi/abs/10.1145/3313831.3376321.

Politou, E., Alepis, E., & Patsakis, C. (2018, March 26). *Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions*. OUP Academic. Retrieved November 21, 2021, from https://doi.org/10.1093/cybsec/tyy001.

Rahman, M. (2018, April 4). *Amidst data scandal, Facebook will voluntarily enforce EU's new privacy rules "everywhere"*. XDA Developers. Retrieved November 21, 2021, from https://www.xda-developers.com/facebook-voluntarly-enforce-eu-privacy-law/.