Takeaways from the GDPR, 5 Years Later: What Worked, What Didn't, and Where Data Privacy and Security Stands

Jennifer Huddleston

May 15, 2023

The European Union's (EU) General Data Protection Regulation (GDPR) became effective nearly five years ago. At the time, much was written about the cost of initial compliance, the impact on companies of a range of sizes, and whether it signaled a shift in the de facto rules for data privacy and security.

With some time having passed and with renewed discussion of federal action in the United States on the issue of data, it is a good time to look at what we can learn from the GDPR, its benefits and consequences, and whether it improved data privacy.

What did the GDPR actually improve?

In general, the key positive of the GDPR is how it overcame a less uniform approach by the EU's member states. This has been particularly recognized in its provision of a strong and uniform data breach law.

The GDPR served to harmonize more laws in a way that created a more uniform standard. However, because the GDPR remains implemented by nation-level data agencies, there remains some differences of interpretation. This can be problematic when dealing with novel data questions in which different data protection agencies may reach different conclusion as to the way the GDPR interacts with an issue or how a single data protection agency in a country may impact the decisions of the whole EU.

Supporters of the GDPR argue that both the increase in data breach notifications and the uniformity that the EU-level regulation provided are superior to the previously piecemeal approach that varied by member state. However, this does not indicate that companies had taken additional steps to prevent breaches or that consumers were necessarily better informed about when their data was breached, but rather there was a more uniform process when this negative incident occurred.

In many ways, the United States is facing similar questions about how a federal law could potentially harmonize an increasing patchwork of state laws, including the 50-state data breach patchwork. A federal law should similarly consider how it could pre-empt or harmonize such

patchworks in the data privacy, breach and security space while still maintaining the flexibility for innovation. But the GDPR also shows the "best" part of overcoming a patchwork must not be considered separately from the potentially problematic consequences the new standard creates.

What problems did the GDPR create or exacerbate?

In the five years since the implementation of the GDPR, several negative consequences for consumers both in Europe and around the world have occurred. In many cases, the GDPR has become the de facto standard—even in countries like the United States that are not covered—as companies find it easier to have a single privacy standard rather than risk non-compliance. Still, the impact of the GDPR is most acutely felt in Europe itself.

First, the GDPR's compliance requirements created new barriers and further harmed the EU's already smaller tech sector, particularly start-ups. While Europe continues to rail against what it views as the problems of America's tech giants, the GDPR only further solidified the competitive advantage such players have in certain markets such as AdTech. More specifically, the GDPR has led to a decrease in the number of apps available in Europe including the introduction of new apps.

Since the GDPR became effective, several websites have chosen to exit the European market rather than engage in costly compliance. This includes not only small players but more household names like the *Los Angeles Times* and Pottery Barn. This is important to note because these companies are not bad actors with unscrupulous data practices, but rather, in many cases, the GDPR made it no longer worth the cost of doing business. These are understandable business decisions, but still leave customers with fewer options even if they were comfortable with the company's data practices.

Beyond these direct elements of the GDPR, the law has also created concerning consequences for innovation and innovative data practices. For example, certain blockchain practices are unable to comply with the GDPR due to requirements around subject erasure, even though blockchain may actually improve data security in some cases. More recently, Italian officials briefly banned popular generative artificial intelligence (AI) tool ChatGPT over privacy concerns and compliance with the GDPR. Innovations like AI, biometrics and blockchain all have the potential to improve data security and data privacy as well as provide new consumer features; however, GDPR restrictions may limit their development and implementation in favor of the status quo.

Did the GDPR actually improve data privacy and security?

Advocates for strong privacy laws may point to Europe as an example to follow; however, there is a lack of evidence that the GDPR actually improved either data privacy or data security. Early on, there were many anecdotal examples of how harsh penalties and strict response times actually led to companies handing over data to the wrong individuals or without truly verifying that it was the individual requesting the data.

While it is easy to attempt to wave off such incidents as merely anecdotal, the average consumer continues to experience the burdens of the GDPR without seeing a real measurable improvement in either their data privacy or data security. Individuals suffer from the fatigue of navigating endless cookie pop-ups and overall increased friction. Studies have shown that there is a lack of evidence to support the idea that the GDPR has increased trust around data collection, while

also showing a decrease in access to online information and retailers as a result of increased friction.

While many may wish that the United States had acted sooner on data privacy and voters on both sides of the aisle favor such action, the GDPR shows the problems that an overly regulatory approach can have and why the United States must carefully consider and strive for a more balanced approach. Even if one argues that strong data privacy and security are worth the tradeoffs to innovation and speech, the GDPR has in many ways failed to achieve its goals, but had significant impacts on innovation and technology well beyond its borders.

Jennifer Huddleston is a technology policy research fellow at the Cato Institute. Follow her on Twitter at @jrhuddles.