Insight

The Price of Privacy: The Impact of Strict Data Regulations on Innovation and More

JENNIFER HUDDLESTON | JUNE 3, 2021

Executive Summary

- While many people value privacy, stringent data privacy regulations have significant economic and other social costs that policymakers should carefully consider.
- Strict privacy regulations place additional burdens on smaller companies and start-ups and have been shown to negatively impact investment.
- Privacy regulations can also negatively impact other benefits for society including free speech, consumer choice, and scientific research.

Introduction

Most people agree personal privacy deserves protection and warrants government regulation in some contexts, particularly on the internet. Privacy does not exist in a vacuum, however, and regulation comes with costs and tradeoffs, particularly with regard to the regulation of online data. As the European Union's (EU) General Data Protection Regulation (GDPR) enters its fourth year and various U.S. states enact their own privacy regulation, the price of privacy regulation has gone from theoretical to very real for a wide range of companies and consumers. Notably, in addition to the anticipated compliance costs, heavy-handed regulations such as GDPR have been shown to have a negative impact on investment in new and innovative firms and on other social priorities such as free speech. As policymakers in the United States consider potential data privacy regulations, they should carefully consider the costs and tradeoffs of such regulations in addition to their benefits.

The Direct Costs of Data Privacy Regulation

The clearest and most easily identified cost associated with more stringent data privacy regulations are those that companies must initially undertake to become compliant. For example, according to a 2017 PwC survey more than 40 percent of responding firms spent over $10 million on GDPR compliance efforts. A 2018 EY and International Association of Privacy Professionals report found companies reported spending an average of $1.3 million per year on GDPR compliance costs. These costs are undertaken not only by European companies but also by U.S.-based companies with an EU presence.

While there are not as many data points available for the California Consumer Privacy Act (CCPA), it would also impose significant initial compliance costs. California's own economic impact analysis found that it would cost California companies $55 billion in initial compliance costs and impact 75 percent of California businesses. This burden would fall not only on tech giants but also on many other industries and businesses including grocery stores and florists. Such costs do not include the burden on out-of-state firms that would also be impacted by the law nor the ongoing compliance costs that are likely to occur.

While the exact compliance costs may vary from proposal –to proposal, the growing number of regulations also brings increasing cumulative costs as companies seek to comply with the nuances of each jurisdiction's requirements. In some cases, companies may be able to use existing compliance mechanisms, but in other cases requirements will likely conflict or have different interpretations requiring development of unique systems. As patchworks of data privacy regulations grow both domestically due to state laws and internationally with various regional laws, the costs of compliance will likely continue to increase.

The Impact of Data Privacy Regulation on Investment and Startups

It is not surprising that many of the costs associated with more stringent data privacy regulation are felt most acutely by smaller companies. Large tech companies including Google and Facebook can more easily absorb the compliance costs associated with more regulatory approaches to data privacy, and thus have seen their market share grow, while smaller online companies have struggled and become less competitive. Additionally, some companies have chosen not to continue to offer their services in certain areas as they find the compliance cost and restrictions too burdensome and costly. For example, companies ranging from newspapers such as the *Los Angeles Times* to email management services to popular stores such as Pottery Barn have all quit offering their online services in the EU following GDPR. It remains to be seen if California will experience any similar issues following CCPA, but such product limitation has already happened in the United States in the wake of other more focused privacy regulation. For example, Google did not offer its art selfie match in Illinois due to the state's stringent biometric privacy law.

While advocates for more stringent data privacy laws often claim they will encourage new more privacy-sensitive companies, the overall impact on the startup sector and venture capital investment appears to tell a different story. While some new and innovative companies have emerged since GDPR was implemented, for example, overall venture capital investment in small and micro companies decreased. A National Bureau of Economic Research (NBER) working paper found that venture capital investment in small and micro companies decreased by $3.4 million per week following GDPR's enactment. This finding is not surprising since investor confidence about such companies' ability to comply, given the costs associated with compliance, has understandably been shaken.

An active and innovative startup sector is important not only to provide competition and improve consumer experience, but also to provide critical economic growth. For example, the NBER study also estimated that GDPR cost 3,000 to 30,000 new jobs due to the decreased investment and startup activity. As the COVID-19 pandemic period has made clear the benefits of innovation as well as the need for continued economic growth, such consequences must be carefully considered.

Tradeoffs Between Privacy and Other Rights

Advocates for strong privacy laws often point to the intangible benefits of privacy or the unquantifiable and often undefined costs of privacy harm. In this regard, they suggest that analyzing economic cost compared to a

rights-based approach may justify the burdens discussed above. Stringent data privacy regulations, however, may also have a negative impact on other rights or societal benefits that are also hard to quantify.

In many cases such regulations are constructed in such a way that presumes increased privacy is the first priority for all consumers; most consumers are not such privacy fundamentalists, however, and instead make a variety of choices that best suit their individual needs and preferences. Current industry-specific regulations as well as market demands illustrate how for certain types of more sensitive information, such as financial or medical information, individuals expect heightened privacy and security standards. For more mundane and often publicly available information, individuals are free to choose more privacy-sensitive options for interacting with their data that may be less personalized or at a cost, yet many individuals still choose to provide their less sensitive data in exchange for a free service or benefit such as a discount. Stringent privacy laws typically presume that regulators know better than consumers what tradeoffs they are willing to make.

It is not just consumer preferences that could be impacted by stringent privacy regulations. Other rights such as freedom of speech and freedom of the press can also be implicated. For example, an EU-style "right to be forgotten" can force the removal of online content and could be abused to silence dissenting voices or journalists . Other concerns could arise as well regarding, for example, the ability to notify consumers during a product recall if companies are limited in their ability to collect or retain certain information.

These tradeoffs are becoming increasingly apparent under GDPR. For example, GDPR stalled 40 cancer studies in collaboration with National Institutes of Health due to data restrictions, and more than 5,000 collaborative scientific studies in 2019 were thwarted by concerns about regulatory compliance. More recently, during the COVID-19 pandemic, there were concerns about the ability to develop contact tracing apps that would comply with the law. More mundane cases also could be snarled in the regulations, from grocery stores seeking to assist the elderly to church prayer lists.

Conclusion

Advocates for stringent privacy regulations point to the value of a right to privacy, but this right does not exist in a vacuum. Analysis of the impact of Europe's GDPR suggests that there is a cost to over-valuing privacy through stringent regulation, both in the economic damage and the tradeoffs to other rights. As policymakers consider potential data privacy regulation in the United States, they should avoid an approach that prioritizes privacy above all else and seek to build on the benefits of the current U.S. approach that focuses on identifiable and quantifiable harms.