Regulatory
Studies Center
THE GEORGE WASHINGTON UNIVERSITY
Improving regulatory policy through research, education, & outreach

Is GDPR the Right Model for the U.S.?

By: Aryamala Prasad | April 3, 2019

At a recent Senate Judiciary Committee hearing, Senator Grassley said, "The European Union [EU] and California have recently taken bold steps to protect data and consumers' personal information. But bold doesn't necessarily mean right." My colleague Daniel Pérez and I have been grappling with the same thought. Is the General Data Protection Regulation (GDPR) the right model for the United States (U.S.)?

To examine this, we employed a benefit-cost framework to identify implications of GDPR-style regulation. The economic costs of GDPR appear to be high in the U.S. as well as the EU. While the strict regulation may be consistent with the EU's stance on fundamental rights, the U.S. context might require applying a more balanced approach that weighs existing evidence of the potential benefits against the costs.

In brief…

Recent discussions on online privacy regulation refer to the European Union's General Data Protection Regulation. It is often seen as a good model to follow for protecting personal data in the digital age. We apply a benefit-cost framework to understand its implications on this side of the Atlantic. Given the existing regulations, an evidence-based approach to identify net-benefits might offer a balanced approach to personal data protection.

Differing Approaches to Privacy

The EU Charter of Fundamental Rights includes the right to the protection of personal data. The EU implemented GDPR to improve the effectiveness of its 1995 Data Protection Directive, which establishes the standards for processing personal data. Although the main aim of the new legislation is to ensure fundamental rights, the regulation also implements uniform laws in all member states to promote the free flow of information within the EU single market. The inconsistent implementation of the 1995 Directive made it difficult for small businesses to work in other member states without incurring penalties.

In contrast, the U.S. protects personal data using sector-specific frameworks in various areas such as health, finance, and children's online privacy. Additionally, Executive Order 12866 requires agencies to "assess all costs and benefits of available regulatory alternatives" and regulate only when evidence suggests that the benefits of a proposed regulation justify its costs. Notably, the benefits of GDPR applied in the U.S. context are not directly evident. We used a benefit-cost framework to understand the implications of applying GDPR at the U.S. federal level. Based on the existing GDPR requirements, we identified the following obligations for businesses:

- Update privacy policies to inform users and require a clear opt-in for using personal data
- Improve IT systems to:

    - Notify users of data breach within 72 hours
    - Provide data in an interoperable format
- Process data subjects' requests for deletion
- Minimize personal data collection
- Designate a Data Protection Officer
- Keep records of data processing
- Conduct impact assessments

Costs and Benefits of GDPR-Style Regulation

Implementing these requirements increases the cost to businesses. First, GDPR increases fixed and variable operating costs, irrespective of firm size. Research suggests the annual IT costs of small businesses can rise by 16 to 40 percent depending on the sector. Further, regulation can reduce investments in tech industries. Data restrictions can also negatively influence trade with other countries. Lastly, depending on the affected sector, regulation can reduce revenues substantially. For example, ad-revenue based businesses such as mobile apps would likely be affected more than subscription-based businesses such as Netflix.

GDPR also has indirect effects on competition and innovation. Large companies such as Google can undoubtedly internalize the compliance costs more easily than small businesses. A large user-base can also help established firms collect personal data whereas these costs could act as entry barriers for small firms. Finally, a study done for the European Parliament indicates that GDPR can create challenges for innovation in big data and cloud computing.

The direct benefits of GDPR differ between the EU and the U.S. In Europe, businesses benefit to the extent the regulation facilitates trade within the internal market. There, a reduction in red tape and clarity in regulatory requirements results in cost savings for businesses that have to comply with GDPR. However, in the U.S., the benefits result from increased trust in businesses because of greater transparency and accountability. For example, Pérez identifies possible benefits to U.S. consumers including: 1) reducing information asymmetry between consumers and businesses, and 2) increasing functionality by allowing users to edit, erase, or transfer personal data.

The details of the above-mentioned costs and benefits would vary for the type of business and the use of personal data. For example, Pérez applied the framework to do a back-of-the-envelope calculation for the mobile apps market in the U.S. His results estimate an annual cost of $24.5 billion in the first year and $5 billion in the subsequent years. The first year estimate includes a one-time cost of compliance for businesses. In comparison, he estimates a potential annual benefit of approximately $8.6 billion in the first year and $6.1 billion in subsequent years.

Overall, GDPR-style regulation could increase the burden on small businesses and restrict innovation. The cost of GDPR is high because it applies to data collection and processing across sectors. In the U.S., existing regulations protect personal information related to health and finance. Expansion of privacy regulation beyond those areas will require better analysis of benefits and costs.

Considering Appropriate Privacy Regulation in the U.S.

Studies by FTC and GAO suggest that consumers are often not fully aware of how companies collect and use their information. These reports suggest a need for greater transparency in information collected and more consumer control over personal data.

Given the existing sector-specific frameworks in the U.S., online privacy regulations could consider what other potential uses of data require more consumer transparency. Discussions on online privacy tend to focus on the use of personal data for behavioral marketing and third-party use. Often, data platforms such as social media or search engines collect personal information, which is passed on to data brokers who sell consumer information. Figure 1 presents example of various data collectors, data brokers, and data users in the personal data ecosystem. U.S. federal regulations already cover data collecting industries such as medical, finance and insurance, and credit card companies. Accordingly, regulators could focus on online businesses such as data platforms and data brokers that are more likely to collect or process personal data.

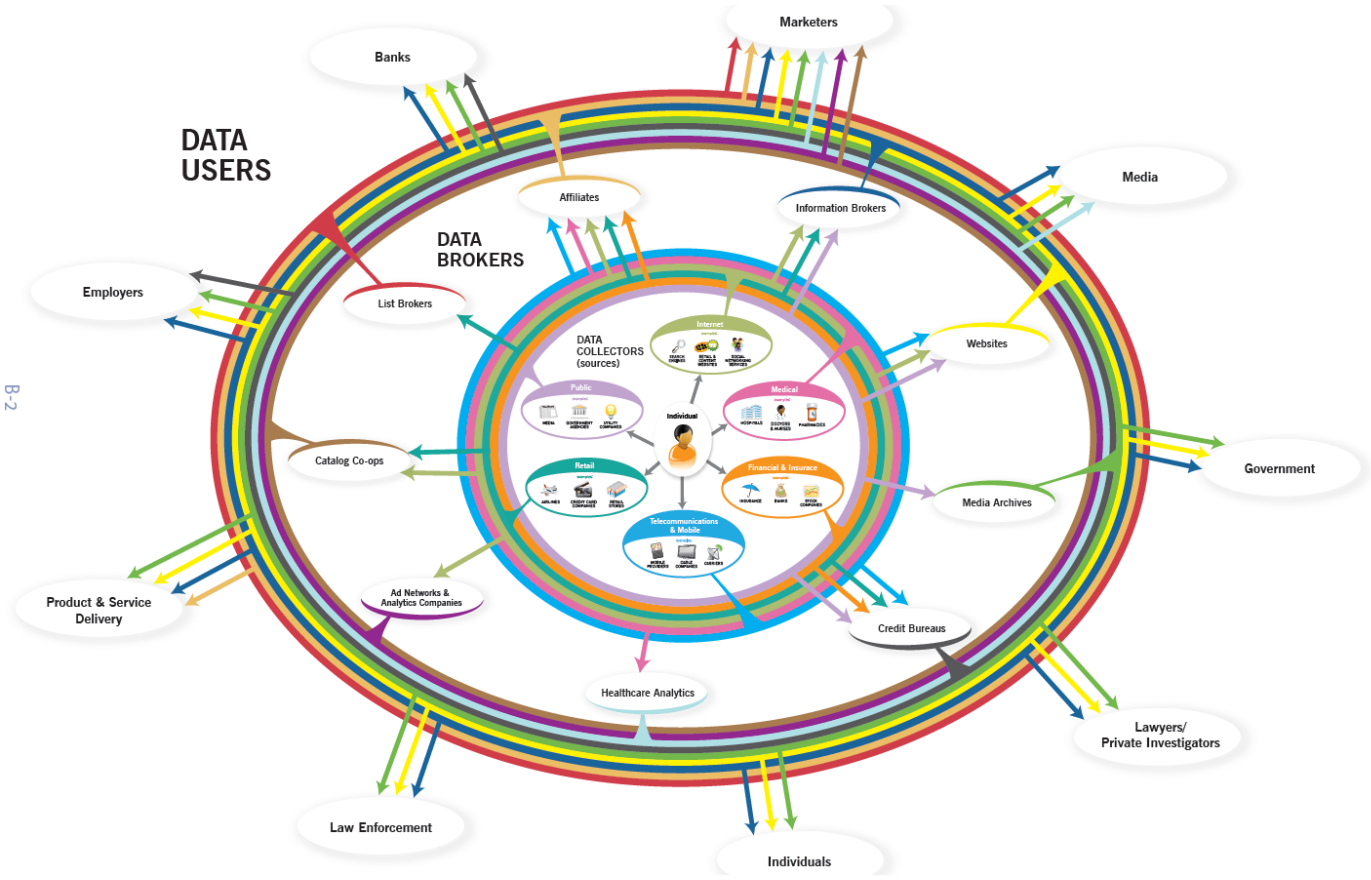

Figure 1: Personal Data Ecosystem

Source: FTC 2012

One challenge in regulating personal data is that some companies need information to fulfill service/product requirements. In a 2012 Report, FTC staff recommended that businesses simplify consumer choice by giving users control over data not required to fulfill a service obligation. In such cases, data practices can focus on full transparency instead of restricting data collection. At the same time, businesses can educate consumers on how personal data facilitates service delivery.

Instead of focusing on GDPR, it might be useful to evaluate current privacy legislation to identify existing sectoral gaps. Policymakers should then consider the benefits and costs of interventions for each sector to inform their policy decisions.

Aryamala Prasad is graduate assistant at The George Washington University Regulatory Studies Center.