Regulatory Studies Center
THE GEORGE WASHINGTON UNIVERSITY

Regulatory Policy Insight
Daniel R. Pérez
July 3, 2019

Privacy Research: The Need for Evidence in the Design of U.S. Privacy Policy

Abstract

It is necessary and feasible for the design of U.S. privacy policy to be based on evidence that policy interventions are likely to increase privacy protections in ways that consumers value. High-quality evidence is one of the most important inputs in the creation of effective public policy. Nonetheless, experts find that oftentimes too little evidence is used to support the policy process—particularly in cases of novel or emerging policy issues. Privacy policy in the digital age of big data and the Internet of things is no exception. This regulatory policy insight details the importance of using evidence to inform the development of U.S. privacy policy and identifies the kinds of evidence that would be particularly useful for policymakers to consider.

Why Privacy Remains a Relevant Issue for Congress

Despite evidence that the costs of intervention may outweigh its benefits, governments have responded to public pressures to regulate the collection and use of consumers' personally identifiable information (PII). For instance, the European Union implemented its General Data Protection Regulation (GDPR) in May 2018; state and local governments in the U.S. have followed suit by establishing similar data protection regimes. Notably, with the California Consumer Privacy Act (CCPA) scheduled to go into effect on January 1, 2020, bipartisan efforts in Congress to create a federal privacy framework are increasing—in part to preempt a "patchwork" of privacy regimes at the state and local levels.

The Importance of using Evidence in the Design of U.S. Privacy Policy

As I mentioned in a public comment to the National Telecommunications Administration, minimizing the burden of unnecessarily duplicative privacy regimes is a reasonable action. However, without a thorough analysis of the potential benefits and costs of the proposals that comprise a U.S. federal privacy regime, the effect on consumer welfare remains unclear. Two points are worth noting here.

First, simply adopting a GDPR-style regime would not be an evidence-based approach to policymaking. Given substantive differences between the EU and U.S. contexts (e.g., the existing regulatory landscape, consumer preferences for privacy protection, market structure, approach to data protection as fundamental right), my colleague Aryamala Prasad argues that GDPR is unlikely

Daniel R. Pérez is a senior policy analyst at the GW Regulatory Studies Center.

to be the right model for the U.S. Studies show that whether social welfare is improved or worsened as a result of privacy policies largely depends on several of these contextual factors.

The EU adopted GDPR in part to update its uniform standards governing the use of PII across all sectors of its single market. Unlike the EU, the U.S. uses sector-specific frameworks (e.g., regulation governing health, finance, etc.) to protect consumer privacy. In addition to sector-specific regulations, the Federal Trade Commission (FTC) uses its authority to bring privacy-related enforcement actions against businesses (e.g., forcing businesses to delete illegally obtained customer data, obtaining civil monetary penalties for violations of privacy rules or deceptive practices that do not conform to a business's privacy policy). These issues span a substantial range of online and offline activities including spam, spyware, peer-to-peer file sharing, behavioral advertising, social networking, and other exchanges of consumer PII. Throughout its history, the FTC has brought hundreds of cases and enforcement actions against companies across various sectors to protect consumer privacy. Policymakers in the U.S. must consider how a federal privacy regime would interact with (or replace) sector-specific frameworks in addition to its effect on the FTC's approach to privacy.

Second, U.S. policymakers should consider evidence on the results of GDPR in the EU. Preliminary analyses suggest that GDPR likely decreased investment in new technology firms, slowed innovation in emerging areas such as artificial intelligence, and reduced competition in the digital market. Notably, GDPR seems to have had the unintended consequence of increasing market share and revenue for larger companies like Google and Facebook at the expense of smaller companies that could not bear its compliance burdens. Although economists have long pointed out that regulation can favor incumbents, this outcome is particularly unfortunate given that the public outcry to regulate is largely the result of data breaches and other mishandling of PII by these larger companies.

The unintended consequence of reduced competition among content providers deserves special attention for at least two reasons. First, competition itself is an effective regulator, lowering the likelihood that companies engage in practices that harm consumers. For example, scholars point out that even in the absence of perfect competition Internet Service Providers are less likely to engage in practices like blocking or throttling (i.e., limiting users' connectivity) if they still "face notable competitive constraints." Second, although its effects are often difficult to quantify, a reduction in the number of high-growth firms entering and exiting the market is likely to hamper innovation (i.e., it may delay the development of the next "Google") given that research finds that these types of firms are generally responsible for a disproportionately large share of economic gains related to growth in productivity, job creation, and GDP.

It is worth noting here that I refer to the aforementioned analyses as "preliminary evidence" because it is too soon to estimate the long-term impacts of GDPR in the EU. The existing results are, nonetheless, instructive for U.S. policymakers as they decide how best to structure federal privacy policy.

Evidence that can Improve Policymaking

Although the literature on data privacy is relatively nascent compared to other subfields in the social sciences, various studies employ clever research designs that generate valid and useful empirical estimates of U.S. consumers' willingness to pay for privacy. The following are specific types of evidence that would be useful for policymakers to consider.

Evidence of Problems: Identifying Privacy Harms and Estimating their Effects

Best practice in regulatory design requires a systematic consideration of evidence early in the policy process to identify which public harms exist and to choose among the various policy tools available for addressing them. Evidence should inform agencies' identification of which forms of intervention are most likely to improve consumer welfare given a particular context. Scholars studying the issue of privacy tend to agree that policy intervention might be an appropriate response if the market does not efficiently allocate resources due to a market failure which—in the case of privacy—occurs for one of two reasons: 1) information asymmetry or 2) externalities.

In the case of information asymmetry, some scholars contend that consumers are not aware of the extent to which companies collect and monetize their PII and, therefore, undervalue their WTP to protect it. According to this line of thought, information asymmetry might explain why studies attempting to estimate consumer WTP generate relatively low valuations—usually somewhere around $1 per month. Similarly, information asymmetry might explain why there is scant evidence of consumer efforts to spend money to protect their PII.

However, a recent survey of 1,599 U.S. consumers asking about their use of Google found that most were aware of the company's data collection and monetization practices (88%) but preferred to share their own PII in exchange for the use of Google's services (e.g., Google Maps, searches on Google.com). In other words, it seems that the benefit these users get from the use of Google's products is at least equal to, if not greater than, the value they attach to their individual PII. Other studies suggest that consumer WTP for privacy is largely dependent on various contextual factors—such as their level of experience with the "Internet of things." Accordingly, the problem of information asymmetry might only apply to a subset of users and for a limited subset of PII. Regardless, policymakers will have to balance evidence of the cost of privacy harms against evidence of the benefits consumers receive from access to the digital economy.

Another rationale for policy intervention stems from the idea that information collection, storage, and sharing often results in harms to consumers whose costs are not borne by companies. For instance, consumer PII could be shared with a content provider who sells access to consumers to advertising companies; at some point the data might be used by (usually unauthorized) third parties (e.g., hackers) which results in harm to consumers. The most pervasive case of this harm is identity theft—where thieves steal login information to bank accounts or credit card information for financial gain. U.S. consumers and businesses incurred an estimated $6.4 billion in losses from

credit card fraud in 2018. It is worth noting here that the type of PII involved in these transactions is usually considered as a separate category of "sensitive" PII (i.e., the difference between your geolocation data—which a hacker might not be able to monetize—and your bank login information—which a hacker is undoubtedly able to monetize).

Finally, in addition to suggesting which forms of regulation may be appropriate, evidence on the characteristics of harms can also inform the decision of whether to pursue *ex ante* or *ex post* regulatory frameworks. *Ex ante* approaches tend either to prohibit or prescribe specific actions whereas *ex post* approaches tend to impose sanctions only on a determination that a harm has occurred—which is often the result of violating a set of principles that define appropriate business conduct. For instance, economic theory suggests that *ex ante* frameworks may be economically efficient to address well-known security risks (e.g., falling prey to becoming part of a malicious botnet) whereas *ex post* frameworks may efficiently address "risks which are contextual, poorly understood…new…and where distribution of harm is difficult to estimate."

The key takeaway here is that evidence related to the characteristics of public harms that result from privacy issues can assist policymakers in going beyond whether "less" or "more" regulation is necessary by informing them which frameworks and forms of regulations are likely to be most effective for addressing particular kinds of privacy issues. Such evidence is a necessary prerequisite for designing policies that benefit the public.

Evidence of Contexts and Characteristics that Affect Consumer Valuations of Privacy

One notable finding that is consistent across the privacy literature is that there exists a substantial degree of heterogeneity regarding consumer preferences for privacy protection. Research indicates that consumer characteristics are not only associated with general attitudes towards privacy (i.e., the extent to which they are willing to pay for more of it) but also of which kinds of protections are valued (i.e., concealing geolocation data vs. concealing browsing history).

For instance, a recent survey of the privacy literature generated the following insights:

- ***Trust* and *Use* were both major factors in consumer valuations of privacy**. Several studies found that users were generally willing to exchange their PII for various benefits but their privacy valuations varied substantially depending on their level of trust in the company that collected and processed their data and on the intended use of the data (i.e., whether it was for academic study or private-sector marketing).
- **Privacy preferences vary for different types of PII**. For instance, women tend to value concealing their geolocation data more highly than men while the latter tend to value concealing their browsing history more highly than women.
- **Numerous additional factors affect consumer privacy preferences**. These include, but are not limited to, country/culture, gender, race, level of technological experience, and age.

These contextual factors make it particularly difficult even for well-designed experiments to generate valid estimates of consumer privacy. In other words, we should be skeptical of the degree to which these estimates accurately capture how consumers value their privacy. Furthermore, the fact that access and use of much of the digital economy is "free"—or, more appropriately stated, provided in exchange for PII which companies then monetize—makes it additionally difficult to generate such estimates.

Nonetheless, even back-of-the-envelope estimates of the benefits and costs of different policy approaches can leverage the best available evidence to generate useful insights on the potential welfare effects of privacy policies. Notably, although estimating the value of privacy is challenging, it is not impossible. In fact, it may be comparable in difficulty to estimations of social costs for other policy issues.

Evidence of the Impact of Policy Interventions

Privacy policy should be informed by evidence that policy interventions are likely to successfully address the problems they are intended to solve. This applies even when evidence indicates that a particular regulatory form or framework is likely suited to address a particular privacy issue (i.e., expecting information disclosure to be an economically efficient method for reducing an information asymmetry). Research on the design of information disclosures points out that they are not all created equal. For example, the Consumer Financial Protection Bureau tested different drafts of its mandated mortgage disclosures on consumers and found opportunities to simplify language and improve clarity to improve their effectiveness. Here, using evidence-based design and testing was essential to ensure that consumers were likely to benefit from reading disclosures—rather than being confused or misled by them.

Problematically, studies find that most consumers do not read privacy policies or terms of service—generally finding them a nuisance. Although privacy frameworks like GDPR mandate the use of "best practice simplification techniques" for disclosures, research finds the use of such techniques to "have little or no effect on…comprehension of the disclosure, willingness to share personal information, and expectations about…rights." This is a particularly relevant example of how evidence can correct preexisting beliefs that certain regulatory approaches will be effective for addressing privacy concerns. If complex disclosure requirements are ineffective or ignored altogether, their use is likely to impose costs on society without generating commensurate benefits. Even worse, mandating burdensome (and ineffective) disclosures often creates an unintended outcome where consumers become fatigued and cynical towards disclosures, reducing the effectiveness of future disclosures. In short, even seemingly intuitive solutions require evidence that they are likely to be more helpful than harmful.

Conclusion

The design of U.S. privacy policy needs to be based on evidence that policy interventions are likely to increase privacy protections in ways that consumers value. Although high-quality evidence is one of the most important inputs in the creation of effective public policy, oftentimes too little evidence is used to support the policy process. Despite evidence that the costs of intervention may outweigh its benefits, bipartisan support in Congress to create a federal privacy framework is increasing. This regulatory policy insight suggested that simply adopting a GDPR-style framework would not constitute an evidence-based approach and suggested different kinds of evidence that policymakers could use to inform the design of privacy policy such that interventions are reasonably likely to increase.