Precision Regulation for Data-Driven Business Models

Joshua New
Senior Fellow, IBM Policy Lab

Christina Montgomery
Chief Privacy Officer, IBM

IBM

As the digital economy becomes increasingly complex and intertwined with daily life, policymakers around the world are grappling with how to effectively mitigate the risks consumers face online. Now more than ever, the flurry of activity from policymakers highlights how important and challenging this is.

In the United States, Congress debates the American Data Privacy and Protection Act and the Federal Trade Commission considers rulemaking on commercial surveillance and data security.[1] In the United Kingdom, Parliament struggles to develop a suitable privacy framework to replace GDPR.[2] In India, lawmakers withdrew flagship privacy legislation to substantially revise it.[3]

As policymakers work to address these important challenges, they have the opportunity to rethink a fundamental element of the data economy that has not yet been meaningfully addressed in data protection frameworks: different data-driven business models pose significantly different risks to consumers.

IBM recommends policymakers consider two distinct categories of data-driven business models and tailor regulatory obligations proportionate to the risk they pose to consumers. High-risk data-driven business models are those that rely on using consumer data as a revenue stream, also known as external data monetization.[4] Low-risk data-driven business models are those that rely on the use of data to improve a company's operations or products and services, also known as internal data monetization or data valorization.[5]

As this paper will explain, incentive structures and other elements of high-risk data-driven business models create a significantly higher likelihood of causing harm to consumers.

R1%&567!1%,1(A!7!fA5,9&1 ?86,1&66 J2%&/6

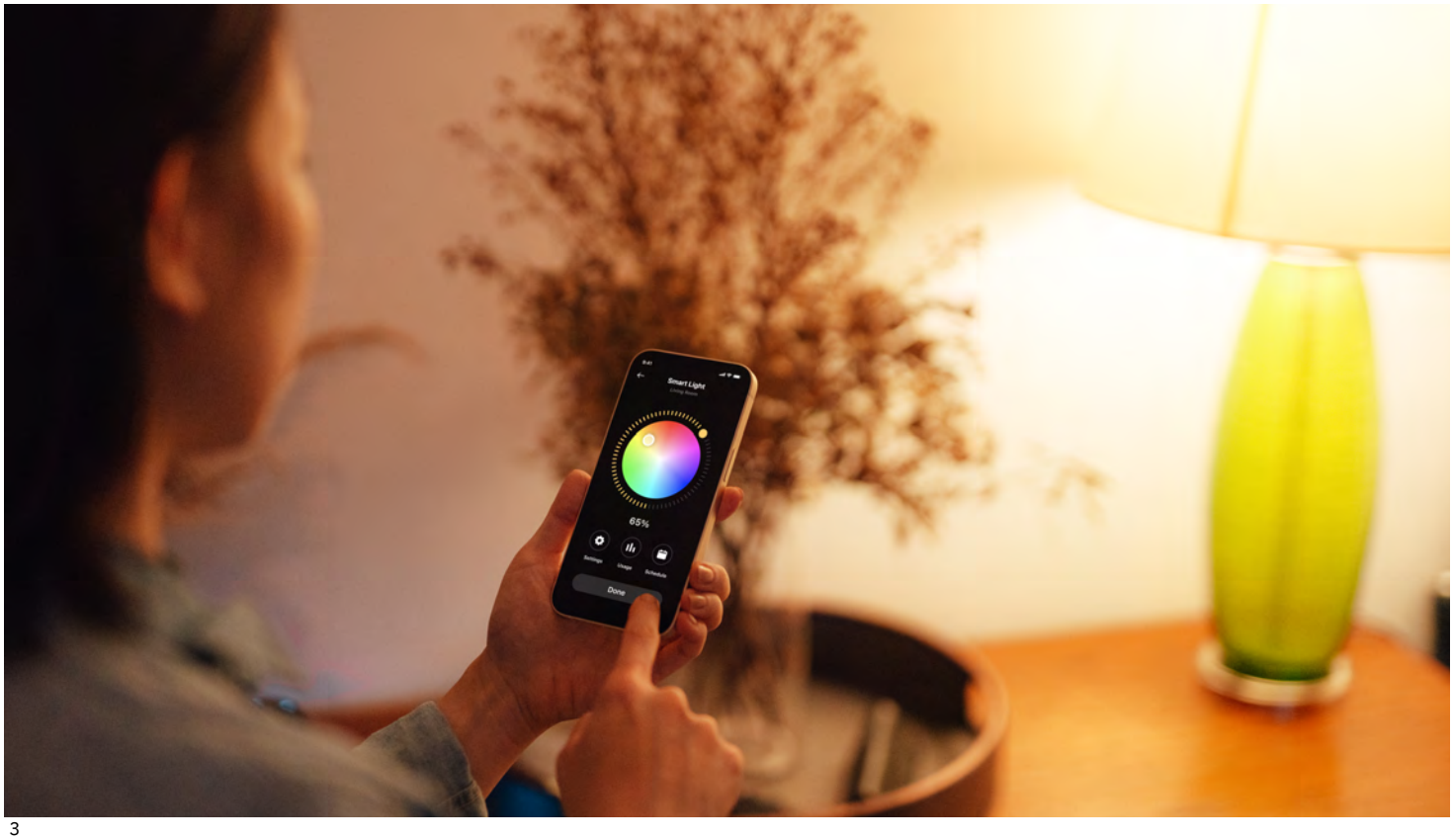
Digital technologies allow consumers to access and benefit from a variety of new and innovative products and services powered by their data. For example, music streaming services can automatically notify users when their favorite bands have scheduled concerts nearby based on their listening history and location data. And credit card companies can use machine learning to analyze a user's transactions, location history, and even use biometric data to prevent fraud. How companies utilize consumer data to deliver these benefits can vary a great deal.

Low-risk data-driven business models have evolved with the advent of digital technologies, but they are not a new concept. Manufacturers, for example, have long used data and feedback from users to improve their products. Modern technologies can make this approach much more accessible and effective for a variety of sectors. For example:

- Company X sells Internet-connected "smart" lightbulbs that monitor and report usage data. Over time, Company X gathers enough usage data to develop an algorithm that can learn customers' usage patterns and give users the option of automatically turning on their lights right before they come home from work.

However, the data collection and sharing technologies that make monetizing data so easy and lucrative did not exist until relatively recently, making high-risk data-driven business models unprecedented in terms of scope, scale, and ubiquity. For example:

- Company Y also sells internet-connected "smart" lightbulbs that monitor and report usage data. Company Y realizes that light usage data is a good indicator for when a person is likely to be home and sells this data to third parties, such as telemarketers or political canvassing groups, that want to target consumers when they are home.

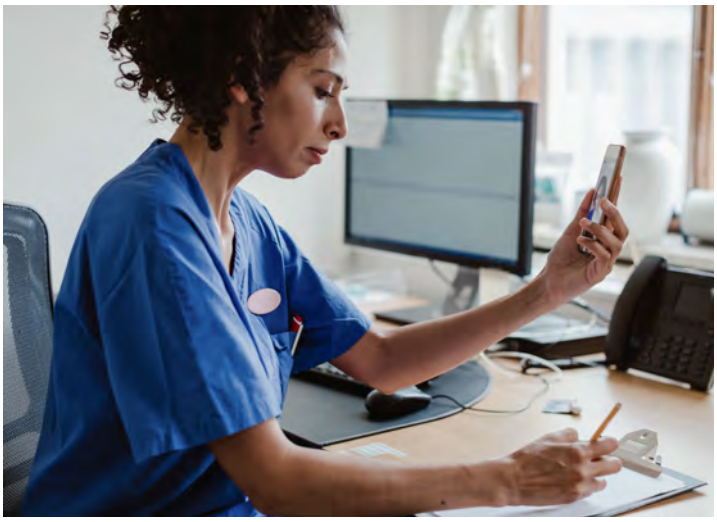


A combination of data protection laws and market forces, such as the potential for reputational damage, can be effective tools to build trust and minimize the risk that data could be misused. However, these tools can be significantly weakened due to the nature of high-risk data-driven business models.

By definition, high-risk data-driven business models exist in multi-sided markets, as a company can only monetize user data if a third party is willing to pay for it. The "long tail" of external data monetization further obscures how a consumer's data is being used, as the initial third party can sell it to another party, which can sell it to another, and so on.

In such cases, consumers have very little, if any, ability to meaningfully understand how their data is being accessed and used throughout the data economy or the level of risk they assume by providing their data. By contrast, in a low-risk data-driven business model, consumers can expect that their data doesn't leave this relationship and can vote with their wallet if unsatisfied with how their data is used and protected. This is a critical distinction.

Importantly, companies that rely on data-driven business models typically have incentives to maximize the amount of relevant data they can access and derive value from. A company with a low-risk data-driven business model will want to access enough data to develop more useful and competitive products and services, but will likely eventually face diminishing returns by trying to access more and more data.



And a company with a high-risk data-driven business model will want to access as much data as it can to sell as much as it can. The incentives to maximize this activity are greater for external data monetization models as a company's success is tied to how much data it can extract from its customers. Such powerful incentives could lead to behaviors that harm or mislead consumers, such as by:

- extracting more data from consumers than they might knowingly be comfortable with, such as by relying on manipulative data collection techniques or "dark patterns;"[6]
- making the value proposition for uses of consumer data opaque and asymmetrical, so consumers cannot easily understand how much their data benefits a company relative to how much they benefit from a company's product or service; or
- obscuring if and how companies share or sell consumer data, such as by relying on opaque and frequently changing privacy policies and terms of service.

Overall, high-risk data-driven business models create conditions in which consumers are more likely to face informational injury and loss of autonomy, while reducing the effectiveness of consumer backlash and reputational damage as a deterrent for bad behavior.

Policy Recommendations

As a global technology company that uses data–and helps clients use data–for a wide variety of different applications, IBM understands the many ways data can fuel innovation and drive social and economic benefits. And as an organization deeply committed to advancing the responsible use of technology, IBM recognizes the need for strong and precise rules to reduce the risk of harm in the data economy. Thus, IBM believes policymakers should rethink how they address risk in data protection frameworks to account for business model risk. Done correctly, this would minimize harm to consumers without hampering data-driven innovation

Just like highly regulated sectors such as health care and education face unique risks when it comes to data that are addressed in sector-specific data regulations, IBM suggests a new approach for policymakers to specifically examine the ways in which different consumer-facing data-driven business models pose different kinds of risks.

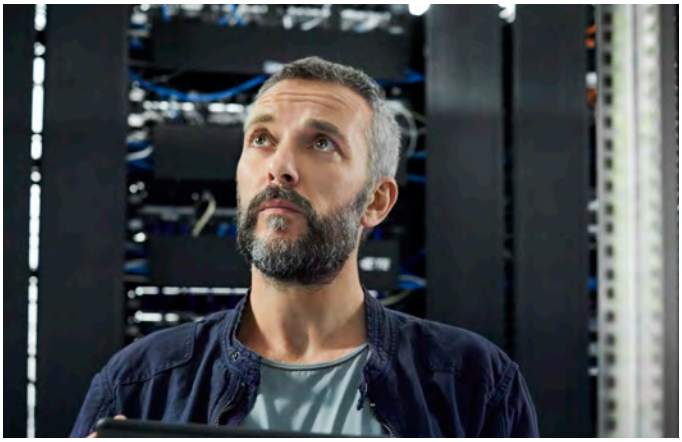
Current consumer data protection frameworks typically do not adequately target high-risk data-driven business models. While notice and consent policies and contractual obligations, such as terms of service agreements, can provide consumers with information on how their data will be shared with third parties, these legal disclaimers can be very difficult to understand, likely do not disclose the identity of third parties, and typically do not govern the "long tail" of data reselling.

Furthermore, even with such frameworks in place, consumers are largely unhappy with how their data is used by companies and believe it to be a "necessary evil."[7] Not only does this cause consumer harm, but it undermines consumers' faith that the data economy is beneficial, rather than predatory.

Identifying the correct strategies to mitigate differences in business model risk will be challenging but failing to act will contribute to the erosion of consumer trust in the data economy and threaten the significant social and economic benefits it can generate. At the same time, heavy-handed, overbroad regulation that does not precisely target these risks would have a similar deleterious effect, restricting low-risk data-driven business models and limiting the potential benefits of the data economy.

Getting this balance right will hinge on whether, and how effectively, policymakers and other stakeholders can advance **seven key goals** related to business model risk:

- Adjust the regulatory burden imposed by data protection frameworks to be commensurate with the risks associated with different data-driven business models;
- Align any rules related to business model differentiation with data protection frameworks that already distinguish between data controllers and data processors;
- Determine whether and how business model risk changes based on whether the data in question is personally identifiable;
- Improve how the levels of risk associated with different data-driven business models can be conveyed to consumers, particularly considering the difficulty in quantifying potential harms;
- Increase transparency into the "long tail" of data reselling, such as by requiring companies to disclose to consumers whether they are selling or otherwise charging for access to their data;
- Require companies that sell consumer data to ensure that their customers buying consumer data act responsibly, and require companies that buy consumer data verify that this data is being collected and shared legally and transparently;
- Promote better understanding of how companies manipulate consumers into sharing data that they would otherwise be comfortable with, and restrict the methods used to do so.



Conclusion

The ways companies utilize consumer data are constantly evolving. As such, implementing new data protection rules prematurely, or in ways that could unduly restrict beneficial innovation in the future, would be unwise. And while many companies can and have used data responsibly for years, policymakers should also recognize that the explosive growth of business models that rely on external data monetization poses serious risks not sufficiently addressed by existing policy frameworks.

IBM strongly encourages policymakers to solicit input from stakeholders in the data economy, including business, consumers, and civil society, about how to best augment data protection frameworks accordingly. As policymakers around the world develop data privacy rules, acknowledging and addressing business model risk will be critical to enhancing consumer welfare.

Sources

1. https://www.congress.gov/bill/117th-congress/house-bill/8152/text;

   https://www.ftc.gov/business-guidance/blog/2022/08/ftc-undertakes-inquiry-commercial-surveillance-practices-wants-your-insights
2. https://techcrunch.com/2022/10/03/uk-data-reform-bill-replace-gdpr/
3. https://www.nytimes.com/2022/08/04/business/india-data-privacy.html

   https://indianexpress.com/article/technology/tech-news-technology/data-protection-bill-revised-penalty-up-to-rs-200-crore-if-firms-dont-have-safeguards-8270461/
4. https://sloanreview.mit.edu/article/demystifying-data-monetization/
5. Ibid.
6. https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf
7. https://www.pwc.com/us/en/tech-effect/cybersecurity/trusted-tech.html