Spotlight 7.1

Understanding the interface between data protection and competition policy

While respecting the prime objective of protecting individuals' data rights, data protection provisions can be designed to minimize the effects on competition and innovation.

Data protection regulations are essential for safeguarding individual welfare and building trust. Yet complying with data protection obligations can also raise the costs of entry and operation for firms—especially smaller firms.[1] Data protection policies that reduce the incentives to share personal data or restrict the use of personal data that a firm has not collected can further entrench incumbent positions and reduce opportunities for innovation.[2] This is not to say that concerns about competition should override the need to safeguard individuals' data rights; rather, there is scope to review the design of data protection regimes to minimize the adverse impacts on competition while continuing to respect data rights.

Evidence from a study of 27,000 top websites found that the General Data Protection Regulation (GDPR) had the unintended consequence of increasing concentration in the web technology sector, with small web technology vendors losing the most market share. This also had the effect of making personal data collection more concentrated after the GDPR was instituted.[3] In these settings, differentiating regulatory treatment between firms according to their size or age may be an option to consider, subject to taking steps to maintain the data rights of individuals.[4]

On the other side of the coin, there is growing agreement that a firm's offering on protection of user data has value to consumers and could be considered a nonprice outcome of competition. Understanding the extent to which firms voluntarily provide enhanced data protection in order to compete becomes important for an accurate analysis of market dynamics.

In the first abuse-of-dominance case relating specifically to data protection lodged by the German competition authority against Facebook in 2019, one question raised during the appeal process was users' willingness to pay for enhanced data protection.[5] However, evidence on the valuation that individuals attach to data protection in different markets is mixed. Some evidence suggests that individuals' stated preferences for data protection often do not match their revealed preferences in practice.[6] Rather than implying a lower valuation of privacy, the issue may be that data subjects (and even the firm collecting the data) do not fully understand how data collected may be used in the future, given the complexity of big datasets and firms' data protection policies.

Moreover, data spillovers may complicate matters. If a platform holds sufficient data on a group of people to allow inferences to be drawn about individuals who have not yet contributed data, those individuals may perceive that they have already lost the power to protect themselves and therefore volunteer data despite their privacy concerns. Such issues may be exacerbated in low- and middle-income countries, where literacy rates, exposure to digital business models, and choice between firms are lower.

Only scarce evidence exists about data protection preferences in lower-income countries. The Data Confidence Index indicates that concerns about the impact of the internet on "personal privacy" appear strongest in Africa, Asia, and the Middle East, while respondents in Latin America generally express higher levels of concern about how companies are using their personal data.[7] Results from experiments in India and Kenya found that customers prefer digital loan products with more "data privacy" features.[8] However, low-income groups who are price sensitive

may be more willing to obtain "zero" price products or services by relinquishing their data.

Overall, there is room for improved cooperation between competition authorities and data protection authorities. Collaboration between regulatory agencies can help policy makers to understand which type of ex ante data protection policies minimize distortions to competition; how to develop appropriate data-focused competition remedies while ensuring data protection; and which antitrust cases to pursue where there may be a link to excessive data collection or exploitation of consumers.

Notes

1. Gal and Aviv (2020).
2. Examples include requiring firms to monitor compliance with the data policy of firms with which they have shared data or limiting the use of data to the purposes for which they were originally collected.
3. Batikas et al. (2020). This increase likely occurred because, after the GDPR became effective, in order to reduce compliance risks, websites (including those that served citizens outside the European Union) reduced their connections to technology providers, especially regarding requests involving personal data. See Johnson, Shriver, and Goldberg (2021).
4. For example, the GDPR allows businesses with fewer than 250 employees to have a limited number of exemptions for recordkeeping (EU 2018). Likewise, in the United States, the Privacy Rule of the Health Information Privacy and Accountability Act does not apply to health plans with fewer than 50 participants that are administered solely by a single employer. See Health Information Privacy, US Department of Health and Human Services, Summary of the HIPAA Privacy Rule (dashboard), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.
5. Colangelo (2019).
6. However, this evidence typically comes from experiments that apply to specific types of personal data in specific contexts and thus makes extrapolations to other settings difficult. See Gerber, Gerber, and Volkamer (2018) and OECD (2020).
7. The Data Confidence Index is constructed from the privacy-related concerns expressed by 391,130 respondents ages 16–64 during the Q1–Q4 waves of research conducted by GlobalWebIndex in 41 countries in 2018 (Datum Future and GWI 2019). Respondents are representative of the online populations of the markets covered.
8. Fernandez Vidal and Medine (2019).

References

Batikas, Michail, Stefan Bechtold, Tobias Kretschmer, and Christian Peukert. 2020. "European Privacy Law and Global Markets for Data." CEPR Discussion Paper 14475, Centre for Economic Policy Research, London, March 2020. https://cepr.org/active/publications/discussion_papers/dp.php?dpno=14475.

Colangelo, Giuseppe. 2019. "Facebook and Bundeskartellamt's Winter of Discontent." *CPI EU News* (blog), September 23, 2019. Competition Policy International, eSapience Center for Competition Policy, Cambridge, MA. https://www.competitionpolicyinternational.com/facebook-and-bundeskartellamts-winter-of-discontent/.

Datum Future and GWI (GlobalWebIndex). 2019. "The Data Confidence Index." Report, Datum Future, London. https://www.datumfuture.org/wp-content/uploads/2019/09/Data-Confidence-Index-Datum-Future-and-GWI-2019.pdf.

EU (European Union). 2018. "Recital 13: Taking Account of Micro, Small, and Medium-Sized Enterprises." *GDPR.EU,* November 14, 2018. Proton Technologies, Calgary, Canada. https://gdpr.eu/recital-13-taking-account-of-micro-small-and-medium-sized-enterprises/.

Fernandez Vidal, Maria, and David Medine. 2019. "Is Data Privacy Good for Business?" CGAP Focus Note, Consultative Group to Assist the Poor, Washington, DC, December 2019. https://www.cgap.org/sites/default/files/publications/2019_12_Focus_Note_Is_Data_Privacy_Good_for_Business_1.pdf.

Gal, Michal S., and Oshrit Aviv. 2020. "The Competitive Effects of the GDPR." *Journal of Competition Law and Economics* 16 (3): 349–91. https://doi.org/10.1093/joclec/nhaa012.

Gerber, Nina, Paul Gerber, and Melanie Volkamer. 2018. "Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior." *Computers and Security* 77 (August): 226–61. https://doi.org/10.1016/j.cose.2018.04.002.

Johnson, Garrett A., Scott K. Shriver, and Samuel G. Goldberg. 2021. "Privacy and Market Concentration: Intended and Unintended Consequences of the GDPR." Paper presented at the American Economic Association and Allied Social Science Associations 2021 Virtual Annual Meeting, January 3–5, 2021.

OECD (Organisation for Economic Co-operation and Development). 2020. "Consumer Data Rights and Competition: Background Note." Document DAF/COMP(2020)1, Competition Committee, Directorate for Financial and Enterprise Affairs, OECD, Paris, April 29, 2020. https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf.