NETWORK LAW REVIEW

ARTICLE

Do our Privacy Laws Strengthen the Already Strong?

Michal Gal

***

The rise of the data economy increased concerns that some uses of data will infringe privacy and harm human dignity. Accordingly, privacy and data protection laws, which place limits on the right to collect, store, or use personal data, play an essential role in such an environment. The rise of the data economy increased concerns that some uses of data will infringe privacy and harm human dignity. Accordingly, privacy and data protection laws, which place limits on the right to collect, store, or use personal data, play an essential role in such an environment.

But have our data protection laws struck the right balance between human dignity and the efficient operation of our data-based markets? This short essay points to some empirical evidence, as well as theoretical reasons, why the current leading model of data protection law might have missed the mark, and instead strengthens the already strong market players and increases concentration beyond what is optimal for social welfare. This claim will be exemplified by reference to the European General Data Protection Regulation (GDPR) and the Californian Consumer Protection Act (CCPA), both of which are relatively recent. This short essay will also suggest some tools that can be used to remedy at least some of these effects.[1]

The complex relationship between data protection and competition

The relationship between data protection and competition is a complex one. Some aspects are complementary. For example, competition over consumers might increase the level of data protection offered by market players. Other aspects, however, create a tradeoff.

[1] Largely based on Gal and Aviv, The Competitive Effects of the GDPR, Journal of Competition Law and Economics (2020)

Intuitively, the stronger the level of data protection, the weaker the competition in data and data-based markets. This is because data protection laws limit internal data flows within a firm (e.g., limiting data exposure to a need-to-know basis), and limit possibilities for data exchanges among market players (e.g., by creating hurdles to data sharing). Limitations on data sharing can strengthen consumer lock-in and increase switching costs, thereby reducing competitive pressures. They can also limit data synergies that may lead to better products. Yet the relationship is much more complex, given that data protection may increase trust in markets and raise users' willingness to voluntarily provide their data and at lower cost.

The story does not stop here. Another dimension of the relationship explores which firms will benefit more from the type of legal regime chosen to further both data protection and competition. Such benefits can result from legal hurdles to data processing and sharing which create comparative advantages to some firms, or from the potential created by the specific law for the use of privacy considerations to justify otherwise anti-competitive conduct. This essay focuses on this dimension.

Current Leading Model: GDPR

The GDPR is currently a leading model around the world for data protection. Other jurisdictions, outside the EU, have also chosen to adopt relatively similar regulation. For example, the Californian CCLP- while different in some aspects – largely resembles the GDPR. Other US states, as well as the Federal government, are also debating whether to adopt a similar law. China has also recently published a Draft Personal Data Protection Law which partly resembles the GDPR. Yet its scope of application may be narrower than in the EU, as protecting personal data is not the only or the overriding objective, and the processing of data can be justified on public interest grounds.[2] Other examples of jurisdictions which have adopted a GDPR-like law include Brazil, Australia, Japan, South Korea, Thailand, Chile, New Zealand, India, South Africa, and Canada.[3]

The GDPR seeks to protect data subjects from harms resulting from unauthorized and excessive use of their personal data in ways which might negatively affect human dignity and well-being. To do so, data processing must comply with several principles. These include lawfulness, fairness, and transparency (e.g., data collection and use must be based on predefined justifications such as data subject's consent), purpose limitation (data must only be collected for specified, explicit, and legitimate purposes), data minimization (collection limited to what is necessary in

[2] Emch, "Antitrust and the internet: is China different?" (2019) 15(2) Competition Law International 167.

[3] Simmons, 12 Countries with GDPR-Like Data Privacy Laws (January 21, 2021), https://insights.comforte.com/12-countries-with-gdpr-like-data-privacy-laws.

relation to the purposes), accuracy, storage limitation, integrity and confidentiality (ensuring appropriate security of the data), and accountability.

To comply with these principles, firms must adopt safeguards, such as technological systems that regulate internal data flows, and verification of GDPR compliance of external data-related contractors.

How does the current leading model affect competition?

Empirical studies have pointed to the potential negative effects of the GDPR on competition and investment.[4] Some of these effects were expected, and were regarded as part of the price to be paid for protecting users' dignity. Yet the debate surrounding the adoption of the GDPR clearly indicates that the magnitude and breadth of such effects constitutes an unintended and unheeded welfare-reducing consequence. Rather, the competitive dynamics created by the GDPR increased concentration in data and data-based markets and reduced the ability to create data synergies among different firms.

Some effects are straightforward. Let me enumerate four such effects. First, the costs involved in organizing a dataset in a way which complies with the GDPR may be high and are characterized by economies of scale. Accordingly, small entrants might find it unprofitable to collect data. Second, the GDPR prohibits or makes it more difficult to engage in some methods of data collection, creating comparative advantages to some data controllers. For example, the need to receive a user's consent to use his data imposes transaction costs for internal data collection, whose effects fall disproportionately on less diversified or new firms.[5] Both dynamics reduce the number of potential competitors in data collection. Third, the GDPR reduces the economic incentives of firms to share any data collected. This is because those sharing data are still liable for monitoring its use by anyone with whom the data is shared. This, in turn, further reduces competition in data supply. Fourth, even where data is shared, the GDPR may limit its use. To illustrate, it is often costly, and sometimes impossible, to obtain informed consent from data subjects to have their data shared with a third party. This effect is strengthened in a multi-product and/or multi-service environment, in which consent is required for each different use of the data. The stronger the legal limitations on using data collected by an external entity, the stronger the comparative advantage for those who can easily collect and use it internally.

[4] For a combined source of such studies see, e.g., Center for Data Innovation, Chivot and Castro, What the Evidence Shows About the Impact of the GDPR After One Year (June 17, 2019); Michail Batikas et al., European Privacy Law and Global Markets for Data (2020).

[5] Campbell, Goldfarb, and Tucker, Privacy Regulation and Market Structure, 24(1) Journal of Economics & Management Strategy 47 (2015).

Other effects are less obvious. To illustrate, the costs of non-compliance include not only the size of fines. Rather, non-compliant data can be viral. Should such data be transferred from an external data controller and combined with the receiver's data, the whole dataset could be polluted (i.e., considered non-compliant). Furthermore, even if the dataset can be separated ex-post, any learning by an algorithm based on the combined dataset cannot be easily reversed, especially if such learning was already incorporated into products or services. Undoing such effects could significantly disrupt business operations. To avoid such consequences, data receivers must engage in ongoing monitoring of their data suppliers' collection and processing practices. This, in turn, might further reduce incentives to use externally collected data, and strengthen incentives for internal data collection. In addition, discussions surrounding the adoption of a data protection law could have an indirect effect on data subjects, who might be more willing to provide their data to larger, more reputable firms, or to firms with which they must interact, at least until the trust of data subjects in the actual enforcement of data protection obligations is increased.

Another type of less obvious effect relates to changes in the policies of dominant firms with regard to third-party access to their data, which were triggered by changes in a data protection regime. The recent change in Google's policy towards the use of third-party cookies is often cited as such an example.

The cumulative effect of such dynamics is a decline in competition in data and data-based markets. The GDPR increases the costs of and barriers to data processing, thereby reducing the number of potential data collectors. Furthermore, it is now substantially more difficult for firms to realize data synergies through data sharing. This, in turn, creates more concentrated market structures and entrenches the market power of those who already enjoy data-based advantages or can more easily collect data by themselves. Such effects belie the confidence expressed by European Commissioner for Justice, Consumers and Gender Equality, according to whom "the big guys increasing market share? I don't believe [the GDPR] will have such a consequence."[6]

Such dynamics offer partial explanations for some of the troubling empirical evidence regarding investment in data-driven markets following the adoption of the GDPR.[7] One study, for example, found that 58% of mergers and acquisitions professionals surveyed reported having worked on transactions that did not go

[6] Schechner and Kostov, Google and Facebook Likely to Benefit from Europe's privacy crackdown, WSJ (April 23, 2018), https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324.

[7] Chivot and Castro, supra.

through due to concerns about the parties' compliance with the GDPR.[8] Another study found that, post-GDPR, the number of deals involving EU ventures with data-related business activities decreased by almost 31%.[9] Another study, which followed more than 110,000 websites for 18 months, documented a substantial shift in market power. With the introduction of the GDPR, the dominant firm in many markets for web technologies, Google, increased its market share.[10] Some of these dynamics have long-term effects.

So- what can be done?

An important element of any solution is awareness. The effects of a data regime on the operation of markets must be carefully analyzed and taken into account in reaching the correct balance. Time here is of the essence, for two main reasons. First, given the positive feedback loop between the size and quality of one's database and entrenched market power, the longer incumbent dominant digital firms will enjoy comparative advantages in data collection and usage, the higher the barriers to entry into their markets. Second, many jurisdictions are currently debating their data protection regimes. Such regimes create externalities on each other. International firms may choose to create a unified internal system of data protection, which is based on the most restrictive law, thereby voluntarily applying such restrictions to other jurisdictions with whom they trade; Government might choose to follow such restrictions, should their firms otherwise be blocked from trading with the jurisdiction with the stricter rules; and ideological ideas flow across borders, pushing governments to adopt laws that are applied elsewhere, sometimes without a serious debate. This is not to say that data protection is not important- but rather that a holistic view of its effects is necessary in order to ensure that we reach the balance which best serves social welfare.

To counter some of the negative effects on competition, some changes might need to take place. Competition law should give more weight to factors which might balance the negative effects of the GDPR on competition and innovation. For example, when evaluating the competitive effects of a merger or a joint venture, more weight should be given to considerations such as the ability of firms to engage in welfare-enhancing data sharing which may facilitate reductions in market concentration, or the potential for significant data synergies that could not be realized otherwise. This implies, for example, a more lenient policy towards

[8] Merrill Corporation, GDPR Burdens Hinder M&A Transactions in the EMEA Region, According to Merrill Corporation Survey (November 13, 2018), https://www.merrillcorp.com/us/en/company/news/press-releases/gdpr-burdens-hinder-m-a-transactions-in-the-emea-region.html.

[9] Jia, Jin, and Wagman, The Short-Run Effects of GDPR on Technology Venture Investment (May 22, 2020).

[10] Peukert, Bechtold, Batikas, and Kretschmer, European Privacy Law and Global Markets for Data (June 29, 2020), https://ssrn.com/abstract=3560392

cooperations between small or medium-sized data controllers, which would enable them to reach economies of scale and scope in data analysis and compete more effectively with those that already enjoy such economies. It also implies that when at least one data controller already possesses strong comparative advantages in data analysis, a careful balance is required between the benefits of increased data synergies and the need to ensure the ability of other firms to effectively compete, in light of the increased hurdles to data collection resulting from the GDPR. The conditions for applying the essential facilities doctrine and granting access to data might also need to be redefined in light of the effects of the GDPR. Importantly, the interface between the GDPR and competition law, in cases where harm to privacy is minimal and benefits to competition and innovation are large, might also need to be reevaluated. In such cases, it might be beneficial not to give GDPR complete primacy but rather to adopt a balancing approach.

In addition, assessments of market power should take into account the actual competitive effects of the GDPR. No longer can it be assumed that new players seeking to accumulate large volumes of data face only low barriers. Furthermore, the actual limits of users' right to data portability under the GDPR should also be acknowledged. It may be difficult for competitors to overcome data-based comparative advantages unless they can convince a sufficiently large number of users to sign up for their services, or unless they can combine different datasets. Yet data portability is limited by user "stickiness," and by the fact that the data potentially arrives in fragmented form and at different points in time.

A final suggestion relates to the structuring of mandatory data-sharing obligations under other laws in a way which is sensitive to the fact that it has become more difficult for small or new firms to grow and enjoy significant data synergies by obtaining data from external sources. To illustrate, some laws facilitate the sharing of some types of governmental data. Such regulations generally do not differentiate between sharing with firms that already possess much data and with those that do not. As argued by De la Mano and Padilla in another context, this may entrench the dominance of the former to the extent that economies of scale exist in the analysis of such data.[11] The above analysis exposes additional grounds for this effect, especially in situations where governmental data can act as a partial substitute for personal data. It might thus be worth considering asymmetric sharing of data so that in certain circumstances the obligation to share data will relate (mainly) to sharing it with small or new entities. In line with this suggestion, it is worth exploring whether more flexible mechanisms for obtaining user consent, such as opt-out rather than opt-in, should be applied with regard to certain types of data.

[11] De la Mano and Padilla, Big Tech Banking (2018).

Michal Gal
Professor and Director of the Center for Law and Technology at the University of Haifa, and President of the International Association of Competition Law Scholars (ASCOLA)..

***

Citation: Michal Gal, *Do our Privacy Laws Strengthen the Already Strong?,* CONCURRENTIALISTE (March 9, 2021).