THE ROLE OF PRIVACY IN COMPETITION POLICY IN DATA-DRIVEN MARKETS

By Prof. (Dr.) Avinash Dadhich & Nidhi Singh
(The authors are with Centre for Competition Law & Policy, GLA University)

Digital environment as such has brought a drastic regulatory and legal transformation that require competition authorities to sharpen their vision during procedures such as merger analysis because of the kind of access tech companies have to data/personal information and trade secrets.

Setting the stage further, we must appreciate that just like competition law has witnessed inherent conflicts with intellectual property rights and consumer law, the current interface with data privacy also raises concerns within the domains of antitrust. The digital economy has made the tension between antitrust and data privacy more pronounced and noticeable wherein you'll notice that if data on one hand fuels competition in the economy, it comes along with a trade off that compromise on privacy. As also rightly argued by many scholars, that there are well developed laws within various jurisdictions that upholds privacy as a matter of right, we echo similar views and would like to bring before you the complex reality that we have seen over the past two decades wherein data privacy law can be seen overall as a separate domain of law in itself.

The digital world today that holds a large amount of Big Data are being shaped by both antitrust and data privacy concerns. Current times is replete with examples of digital platforms like Facebook, Google, Apple and Amazon that have faced the scrutiny of apex antitrust authorities in Asia, America and within Europe for their data-driven competition practices.

Privacy protections can be considered a form of non-price competition that is especially important in industries where services are offered for free (Okuliar 2015). Instances have been seen where firms can compete by offering tighter/or more transparent privacy policies. However, in case of mergers, if the entity becomes dominant, the dominant firm can harm consumers, as it has no incentive to invest in privacy. With the increase in number of Big Data related merger cases, there has been a sharp increase in potential harms that has mainly arisen on account of acquirer getting access to underlying data set of the target company. In our view, antitrust authorities must examine transactions in light if it is also likely to reduce incentives to compete in providing privacy to consumers. For example, in Google Double click case, while rendering a dissenting opinion, then Commissioner had remarked that privacy could be 'cognizable' under the antitrust laws. Transactions under given circumstances could lead to improved product, lower prices or greater innovation on account of resultant data gains.

Erika A. Doughlous (2021) argues that there are two specific area of tension emerging between data privacy and antitrust law in the digital economy. Firstly, the general practice being followed by the tech companies in the platform market is that they tend to invoke data privacy as a business justification to defend against allegations of anti-competitive conduct. Secondly, scholars and agencies have been seen to be calling for remedies that grant access to the data held by digital platforms. Both these concerns have in a way implicated the data privacy interests of the consumers who are exposed to the disclosure requirements without much willingness to do so.

However, what has been seen that competition concerns have mostly over-ridden the role of data privacy. One such example is the recent Ninth Circuit decision of the USA courts in *HiQ v. Linkedin* that provides a description of the new and this inherent tension existing between the two in digital world. In this case, Linkedin terminated HiQ's access to user profile data on the Linkedin social network arguing that HiQ violated user privacy settings through its collection and dissemination of profile data in data analytics software. The claim of HiQ that termination was unfair competition and the practice of Linkedin is intentional in terms of ousting a rival. By granting continued to LinkedIn user profile information, what can be seen is that it effectively guaranteed that HiQ could continue to override privacy settings in the name of competition. This also appears to be in contradiction with the approach taken by FTC that wants to ensure privacy law enforcement. Instances like these, begs the question whether antitrust analysis would examine data privacy protection cognizable as a business justification?

The second area that we would like to expand on is the antitrust behavioral remedies that compel, access to personal information held by digital platforms as a means of restoring online competition. Margrethe Vestager, Commissioner of Competition, European Commission has remarked that with data becoming increasingly important for competition, the future isn't too far when giving access to data would be the best way to restore competition (for instance: behavioral remedies that grant rivals compulsory access to user data held by those platforms).

What we have tried to highlight through our discussion is that there is a some sort of 'competition first' approach in cases of conflict between data privacy and antitrust in the platform markets. The reason for this could be the kind of mandate competition authorities are bestowed with i.e to advance competition. Data privacy takes a different course of law in itself. But ideally, the approach that should be followed is --- while encountering with cases that raises data privacy on the horizons of antitrust, a very non-biased and a 'no primacy' approach should be followed. This needs to be done on a case- by- case basis, as also suggested by my co-speaker Mario. Doing so shall involve assessing the importance of respective interests at stake in antitrust and data privacy that should be weighed and considered against each other. The solution could be a more accommodative approach to

handle the interface between antitrust and data privacy and not act bias towards any particular area of law while giving equal billing to both.

The way we see this issue is that they are complementary to each other and must not be dismissed as a separate legal doctrine while dealing with the inherent tensions and interface. The decision should be made in light of the scope of the permitted conduct within the contours of digital platform economy.