Westlaw India

European Competition Law Review

2021

Facebook EU tussle: lesson for big tech

Pratibha Jain*

Payel Chatterjee**

Vinay Shukla***

Dibya Prakash Behera****

Subject: Competition law. **Other related subjects:** European Union. Information technology

Keywords: Australia; Competition procedure; Digital technology; Discovery; EU law; India; Provision of information; Social media

E.C.L.R. 111 The last few months have been particularly interesting in the international antitrust landscape, for it is the first time that a private company has locked horns with the European Union's ("EU") antitrust watchdog, the European Commission ("EC") over the relevancy of information sought by the EC in the course of its investigation. Having already been subjected to intense scrutiny of different antitrust regulators around the globe and their incessant data demands, Facebook ("FB") has finally retorted and stepped up the ante by approaching the European General Court ("General Court") accusing the EC of seeking irrelevant information, including data of a highly personal nature. This complaint comes against the backdrop of the EC's data requests to FB for its investigation and the threat of penalty looming large (daily penalty amounting to 8 million euros) over FB for any non-compliance with such requests. The EC's demand includes documents containing highly sensitive information such as employees' medical information, personal financial documents and private information about an employee's family members. In what can be hailed as a small win for FB, the General Court has temporarily suspended the EC's request for such information pending their response to the FB's concerns.

It is interesting to note that the EC has been at the forefront in conducting antitrust investigations and leading the path in regulating the digital economy by actively investigating many tech companies. Its Indian counterpart, the Competition Commission of India ("CCI") is also not too far behind in tightening the noose around the alleged antitrust practices of tech giants. Lately, it is almost as though an investigation is initiated against a tech giant in India every month. Notable examples include the CCI's recent probes against Amazon, Flipkart, MakeMyTrip and Google. Therefore, it becomes pertinent to pre-empt the road forward for tech giants in such investigations, specifically in the context of FB's allegations against the EC and the General Court's observations.

European Commission: powers to cripple or cause a ripple?

The EC derives its power to investigate and consequently demand documents from the European antitrust policy. The European antitrust policy is developed from two central rules set out in the Treaty on the Functioning of the European Union ("TFEU"). The EC derives the power to implement the rules laid down under arts 101 and 102 of the TFEU from the Council Regulation (EC) 1/2003 ("Regulation").

The EC is vested with wide-ranging powers while launching an investigation, including not only the right to request information from entities, but also to enter their premises, seize records and interrogate their representatives as the EC deems necessary.[1] The Regulation (via art.20) specifically gives extensive power to the EC allowing its members to enter any premises, land and means of transport of such entities, examine their books and other records, take or obtain in any form copies of or extracts from such books or records, seal any business premises and books or records for the period and to ask any representative or member of staff for explanations on facts or documents relating to the subject-matter and purpose of the inspection and to record the answers. While a literal and objective reading of such provisions would suggest that the EC is vested with powers that can virtually go beyond the contours of all laws and regulations in place, in actuality, the Regulation allows such powers to be exercised only for collection of information which is necessary for the purposes of investigation. The innate subjectivity of the word "necessary" may still prove to be detrimental for entities being investigated, as they have no way to ascertain themselves the necessity of the information being provided to the EC.

However, much to the saving grace of the entities being investigated, the Regulation also requires the EC to state the legal basis, specify any other required information and the purpose of such inspection. Except for the aforesaid, the only respite for the entity subject to such inspection or investigation comes in the form of art.18(3) of the Regulation, which allows for entities to have such requests reviewed by the Court of Justice. It is also relevant to note that approaching the General Court for such requests received from the EC could be necesssary not only due to the irrelevancy of the information requested but also because of the increased risk of unintended disclosure of sensitive data which may add to the woes of the company and also the recipient, especially with the General Data Protection Regulations***E.C.L.R. 112*** ("GDPR") and Regulation (EC) 45/2001[2] having laid down stringent provisions[3] for the processing of personal data.

Similar concerns, different jurisdictions

Similar cases across jurisdictions worldwide only reinforce such apprehensions. The concern seems to be twofold: the nature of such data being highly proprietary, sensitive and confidential and the inadequacy of safeguards maintained by the regulators to prevent the disclosure of such information. Some examples can be seen below:

Recently, Google filed a petition in a Texas court to ensure that the state-led probe into possible antitrust violations by the internet search and advertising company does not compromise its confidential business information to any rival parties.[4] Google was seeking a protective order for its "highly proprietary, competitively sensitive, and otherwise confidential" information. This was especially important as the Federal Trade Commission ("FTC") had inadvertently disclosed the FTC staff's internal and confidential report about its 2012 investigation into Google's search engine practices.[5]

In Australia, the antitrust regulator had disclosed confidential information about its decision to block a $10 billion merger of TPG Telecom and Vodafone's Australian joint venture, blaming a flaw in its website.[6]

Similarly, in early 2020, the UK Financial Conduct Authority ("FCA") admitted to a data breach exposing confidential information belonging to roughly 1,600 consumers. The financial watchdog claimed that the information exposure occurred following the public release of data in response to a Freedom of Information Act ("FOI") request. FOI requests can be made in the UK for records held by public authorities. The request at the heart of the data leak was made in relation to how many complaints were made against the FCA—and handled by the authorities' complaints team—between 2 January 2018 and 17 July 2019. When these records were published and made available on the FCA website in a document, the confidential information of complainants, of which there were approximately 1,600 during this timeframe, was also made public.

Relevancy to India and analysis

At the outset, it is important to note that the Indian and EU antitrust regulators have similar powers considering that our regulations have been shaped and inspired by the EU.[7] The Indian antitrust regime is governed by the Competition Act 2002 ("Act") which provides for a host of powers exercisable by the CCI. Pertinently, s.26 of the Act allows the Directorate General ("DG") to conduct investigations and submit a report in accordance with the provisions mentioned thereunder. While conferring such powers, the Act also allows the DG to exercise all such powers as have been vested with the CCI. In particular, the DG, for the purposes of discharging its functions has the power to summon and enforce the attendance of any person and examine him on oath, require the discovery and production of documents, issue commissions for the examination of witnesses or documents, and requisition any public record or document or copy of such record or document from any office. These are similar to the powers under regs 17–28, which entitle the EC to perform similar functions related to the collection of information that is "necessary" for the case at hand. In other words, the CCI can seek any information that it deems necessary for the purposes of investigation including data which may be regarded as highly sensitive and personal. With the introduction of the Personal Data Protection Bill 2019, these issues assume centre stage and deserve due consideration from the CCI even more than previously.

It is interesting to note that these issues have also manifested into case laws. For instance, in JCB India Limited v Competition Commission of India,[8] concerns were raised on the DG conducting search and seizure of hard disks, laptop and materials critical to the investigation from the premises of the petitioners. The petitioners moved an application pleading, inter alia, for quashing the search and seizure conducted by the DG and also to return all the documents, cloned hard drives and laptops seized from their premises during the search and seizure. However, the CCI, striking a middle ground, ordered all such information to be kept in a sealed cover in safe custody. While this case may be differentiated on the grounds of the CCI's balancing approach, the***E.C.L.R. 113*** apprehensions of the petitioner with regard to relevancy and confidentiality of highly sensitive data cannot be categorically ruled out. It will not be surprising to see such claims springing up in the future.

The road forward: some lessons for big tech

FB's encounter with the General Court raises interesting questions about the nature of data required by regulators in the course of an antitrust investigation. In the specific context of personal data being sought for an investigation of antitrust allegations, regulators will be required to demonstrate a visible nexus between the allegations and the need for sensitive personal data in connection with the investigation. In the EU, the GDPR adopts a consent-centric approach, whereby data can generally be transferred only with the knowledge and express consent of the data principal.[9] A violation of these provisions can lead to hefty penalties by the defaulter, often to the tune of millions.[10]

It seems that in the future more and more companies may be concerned about such data requests from antitrust regulators especially due to the highly sensitive and personal nature of data. Given that the General Court has temporarily suspended the EC's request, it may pave the way for such companies to also stop regulators in their quest for data.

The Indian ecosystem, on the other hand, is less developed than the EU. The current data protection law protecting the personal information of individuals lacks teeth in places but is considered adequate and sufficient for the Indian regime from a business perspective. Regulators in India, including the CCI, enjoy unfettered investigatory powers without any adequate safeguards for the handling, use and storage of personal data. One prime example of the same would be the recent investigations into the alleged suicide case of Bollywood celebrity Sushant Singh Rajput, where despite the matter being sub judice and the relevant agency taking all the precautions for storage of personal data, personal Whatsapp messages of the accused and her friends were leaked and used by news channels for a vicious media trial.[11] The Ministry of Electronics and Information Technology's Committee of Experts has also released the Draft Non-Personal Data Governance Framework recently, which affords non-personal data[12] (such as confidential information, business and trade secrets) the same level of protection as personal data. Thus, it may be possible in the near future for enterprises in India to also address relevancy concerns with the Indian regulators and the CCI should consequently be required to make adjustments and/or be highly specific while requesting data from enterprises.

Interestingly, the Central Board of Direct Taxes has recently authorised income tax authorities to share limited information with the CCI.[13] However, the tax authorities have specifically been instructed to form an opinion about the relevance of the information to be shared before they share such information with the CCI as it may contain sensitive financial information of taxpayers. While this is a case of information exchange between statutory bodies and need not apply to information transfer by an enterprise in pursuance of a direction by a regulator, the carving out of "relevance" as a prerequisite to transfer of data seems to be recognised more and more every day. It will assume greater significance in the future and needs to be analysed on a case-by-case basis.

Pratibha Jain

Payel Chatterjee

Vinay Shukla

Dibya Prakash Behera

E.C.L.R. 2021, 42(2), 111-113

*. Partner at Nishith Desai Associates (NDA), an India Centric Global law firm with offices in Mumbai, Palo Alto (Silicon Valley), Bangalore, Singapore, New Delhi, Munich, and New York.

**. Head, European Practice at NDA.

***. Senior Member, Competition Law Practice at NDA.

****. Associate, Funds Formation & Regulatory Practice at NDA.

1. Implementing EU competition rules: application of arts 101 and 102 TFEU, art.101, https://eur-lex.europa.eu/summary/EN/legissum:l26092 [Accessed 4 December 2020].
2. Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001R0045 [Accessed 4 December 2020].
3. GDPR art.84 and Irish Data Protection Act 2018 s.141, https://data.oireachtas.ie/ie/oireachtas/act/2018/7/eng/enacted/a0718.pdf [Accessed 3 December 2020].
4. *Tony Romm, "Texas, Google battle over experts in states' antitrust probe" (18 December 2019) The Washington Post*, https://www.washingtonpost.com/technology/2019/12/18/texas-google-battle-over-experts-states-antitrust-probe/ [Accessed 4 December 2020].
5. *Brody Mullins, "Inside the U.S. Antitrust Probe of Google" (19 March 2015) The Wall Street Journal*, https://www.wsj.com/articles/inside-the-u-s-antitrust-probe-of-google-1426793274#:~:text=Inside%20the%20U.S.%20Antitrust%20Probe%20of%20Google%20Key,services%20over%20rivals%E2%80%99.%20WSJ%E2%80%99s%20Matthew%20I [Accessed 4 December 2020].
6. *"Australia regulator blames website flaw for early reveal of TPG-Vodafone decision" (16 May 2019) Market Screener*, https://www.marketscreener.com/TPG-TELECOM-LTD-9058858/news/Australia-regulator-blames-website-flaw-for-early-reveal-of-TPG-Vodafone-decision-28606323/ [Accessed 4 December 2020].
7. *Anu Bradford, Adam Chilton, Katerina Linos and Alex Weaver, The Global Dominance of European Competition Law Over American Antitrust Law (2 July 2019)*.
8. JCB India Limited v Competition Commission of India (2015) 224 DLT 30.
9. GDPR art.6(1)(a) (which requires express consent to be taken from the data principal by processors prior to storing any data. Therefore, it follows that such situations must expressly be contained in any documents where businesses seek to disclose how they are to make use of the data stored).
10. GDPR art.83.

11. *Mehak Sawhney, "Fuelled by Leaked Evidence and Illegal Surveillance, Media Trials the New Normal in India" (9 October 2020) The Wire*, https://thewire.in/rights/leaked-evidence-illegal-surveillance-media-trials-new-normal-india [Accessed 4 December 2020].
12. "Sensitive non-personal data" is non-personal data originating from personal data.
13. *ET Bureau, "CBDT allows income tax authorities to share information with CCI" (31 July 2020) Economic Times*, https://economictimes.indiatimes.com/news/economy/policy/cbdt-allows-income-tax-authorities-to-share-information-with-cci/articleshow/77291049.cms [Accessed 4 December 2020].

© 2021 Sweet & Maxwell and its Contributors

Westlaw India™