FTI JOURNAL

ARTICLE

Can Data Privacy Be a Competitive Advantage?

March 2021

The ambiguity around protecting data and regulatory compliance creates a tension for companies that they must navigate to stay competitive.

The way personal data is collected and used by companies today has gone from a novel strategy to a business imperative. A company's success — or demise — can depend on the kinds of data it maintains and how it utilizes this trove in all aspects of its operations.

As data and data privacy evolve into valuable assets for businesses and consumers, respectively, the collection and use of data have become aspects in which companies can and do compete. This raises a key question in the digital age: Can data privacy be used as a competitive advantage?

Examining existing corporate data practices of companies, independently and as part of significant corporate transactions, helps elucidate how the transference and use of consumer data may give rise to complaints from consumers, competitors and competition authorities. Within the M&A context in particular, these examples make clear that both acquiring and target companies may be on the hook for misuse of data.

As this is an evolving space, it remains unclear how regulators — and ultimately, the courts — can establish clear definitions. To gain an understanding of the issues and provide companies with thoughtful guidance about how their own data usage may implicate competition law, here are three important considerations to take into account.

Data Sharing

How a company shares data often comes down to the circumstances and reasons why personal data can be disclosed. Generally, there needs to be a fair and lawful basis for this disclosure.

Early last year, a major credit card company announced it would be acquiring a tech firm that connects a customer's bank accounts with payment services provider apps such as Venmo and Wise (formerly known as " Transferwise"). The U.S. Department of Justice (USDOJ) stated in November that the firm, in its role as an intermediary between the banks and these apps, would have access to the log-in information and other sensitive data of 200 million consumer bank accounts and 11,000 banks.

Transparency is key

When asking for consumers' consent to use their data, companies have a responsibility to provide full disclosure to consumers on how their data is being used and who has access to the data.

The USDOJ, which filed a civil antitrust lawsuit to block the merger, objected on the grounds that the acquisition would have eliminated a potential competitor to the credit card's market dominance in online debit. Meanwhile, users of Venmo and Cash App filed a class action lawsuit against the tech firm, claiming it violated the privacy rights of millions of customers. In the face of these challenges, the companies abandoned the transaction.

Key Takeaway: Taking possession of another firm's data presented the credit card company with a competitive advantage to connect with a rich ecosystem of banks and accounts. Even if the deal had gone through, however, European privacy issues might have prohibited the company from using the acquired data lawfully.

Data Use

In an M&A context, even where the target company is legally authorized to transfer consumers' data, the competition authorities may feel it necessary to regulate the use of that data.

In 2019, regulators and consumers alike raised questions about how a multinational tech company might use private data housed by a fitness company in a proposed acquisition. Authorities in the European Union (EU) were particularly concerned that the data would give the multinational an unlawful competitive advantage while obscuring its use from consumers to whom the data belonged, in violation of the EU's General Data Protection Regulation (GDPR).

Setting aside the GDPR issues, the European Commission's Directorate-General for Competition focused on how the multinational could use the data to potentially bolster its ad business while restricting access to competitors. Eventually, the European Commission granted antitrust approval for the deal after the multinational offered concessions to restrict its use of the data for its ads while continuing to provide access to software applications through the fitness company's Web application programming interface (API).

When evaluating the value and appropriateness of a proposed acquisition, the parties should consider:

- Will the acquirer use data for the same purpose it was used for by the target?
- If consent is being used as a lawful basis, have you ensured that the consent is transferable? If not, the acquirer may need to renew consent from data subjects before continuing processing with a clean, unambiguous record of that consent.
- Where will the data be stored, processed and transferred post close?
- What data transfer mechanisms will be used to safeguard the data?
- Whom will the data be shared with and are there any data-sharing agreements in place?

Key Takeaway: Although the GDPR and the European Commission treat competition and privacy as separate concerns, both still require considerations of consent, access and tracking usage. All these concerns should be evaluated during the due diligence phase of an acquisition.

Privacy as a Competitive Advantage

When handled right, data privacy can in fact offer a competitive advantage. Take for example, Siemens, the German multinational. It has invested billions in its MindSphere platform, a cloud-based Internet of Things (IoT) operating system that works to help customers cut costs and improve productivity. Siemens believes that by keeping customer data siloed in this way, it is more highly protected than in systems employed by rivals. That heightened

protection is a selling point for Siemens, giving it a potential competitive advantage.

Lawful basis

The acquirer must ensure that the personal data they intend to use was obtained lawfully. Further, acquirers must meet the elevated thresholds required for consent if used as a legal basis. Your collected consumer data is not available to all.

Then again, data privacy can potentially squeeze out competition and set off antitrust alarm bells. Late last year, for instance, the FTC sued a major social networking service, accusing it of "illegally maintaining its personal social networking monopoly through a years-long course of anticompetitive conduct." The FTC cited allegations about the service's earlier acquisition of competitive threats and refusal to provide APIs to apps with competing functionalities. Those functionalities included rival personal social networking services or mobile messaging apps. The FTC further alleged that these actions hindered consumer choice, including alternative personal social networks with privacy protection options.

Key Takeaway: When it comes to data, privacy can be a double-edged sword. On the one hand, it is a tool for protecting consumers. On the other hand, it can be wielded as a weapon against competitors. Privacy controls need to be embedded into the DNA of the business and operational processes to avoid being perceived by consumers as just following the latest "privacy washing" Silicon Valley trend.

Growing Vigilance. Even as the ambiguity between data privacy and anticompetitive behavior causes tension, what remains clear is that regulators are becoming increasingly vigilant about company compliance. The scenario is evolving, and treading carefully is paramount. One false step can not only result in investigation, but alienate customers.

In a speech in late 2019, then Assistant Attorney General for the USDOJ's Antitrust Division, Makan Delrahim, put it this way: "Although privacy fits primarily within the realm of consumer protection law, it would be a grave mistake to believe that privacy concerns can never play a role in antitrust analysis." Woe to the company that does not keep that duality in mind.

SONIA CHENG
Senior Managing Director

FREDERICK HILL
Managing Director

ANDREA B. LEVINE
Managing Director