Bloomberg Law Insights

Enforcement

How Privacy Protections and Data Are Changing Antitrust in Tech

BY DANIEL BIRK, ESQ. AND DEBBIE REYNOLDS

Some experts have speculated that Amazon.com Inc.'s recent bid to buy the organic grocery store chain Whole Foods Market Inc. may be less about gaining a foothold in the brick-and-mortar grocery world and more about gaining access to data: specifically, data about how people shop for groceries and what they buy, in stores and online. (*See, e.g.*, Laura Stevens & Heather Haddon, ''Big Prize in Amazon-Whole Foods Deal: Data,'' Wall St. J., June 23, 2017.)

In the age of big data, personal information has become a huge commodity. The ability to aggregate and analyze consumer data has proven extraordinarily valuable to advertisers and retailers, which use consumer data to improve and target their offerings. Firms such as Google Inc. and Facebook Inc. have translated their access to user data to reap tens of billions of dollars in annual advertising revenue. (*See* ''The World's Most Valuable Resource,'' The Economist, May 6, 2017.)

We live in a digital age where information as vast as oceans creates enormous opportunities for global technology companies to develop unique ways to gain users, leverage their innovations, and monetize personal and private information of consumers. Some of the most dominant and profitable technology companies provide free services to consumers in exchange for the use of their personal or private information which is purchased by marketers who can target advertising to users.

But with that increase in data value has come a corresponding increase in concerns about how businesses use consumer data and how those businesses are — or are not — protecting their customers' privacy. Consumers of many ''free'' popular and convenient internet applications often agree to voluminous (and seldom-read) terms of service that expose their demographic information and online browsing, shopping, or social history to analysis and use by marketers. By saying yes to these terms of service, consumers may rapidly decide that the intrinsic value of the services provided outweigh concerns about data privacy and the use of their information for marketing purposes.

As concerns about data privacy have grown, so too have calls from some quarters to use antitrust and competition laws to rein in acquisitions of or by firms that collect or use consumer data and to impose additional scrutiny on the market conduct of e-commerce companies. A recent *Wired* article highlighted this view, noting a statement by Andreas Mundt, the head of Germany's antitrust agency, that ''privacy is a competition issue.'' (*See* Nitasha Tiku, Digital Privacy is Making Antitrust Exciting Again, www.wired.com, June 4, 2017.) Some have also questioned whether the existing antitrust regulatory framework is sufficient to address unique challenges to competition posed by big data and have contended that competition laws should be expanded or reinterpreted to target data-related concerns.

These proposals, and their responses from regulators in the United States and the European Union, have served to expose fundamental differences of opinion about the role of antitrust in market regulation and how privacy fits into the framework of competition law. Businesses should be prepared to navigate these differing conceptions but should not, at this point, anticipate that competition authorities on either side of the Atlantic will radically revise existing antitrust laws to carve out a special place for privacy concerns.

Differing Views in U.S., EU

The European Union's demands that multinational businesses better protect the privacy of their users' information have grown increasingly louder in recent years. In 2015, the European Court of Justice invalidated the 15-year-old Safe Harbor Framework Agreement between the European Union and the United

Daniel D. Birk is a partner at Eimer Stahl LLP, where he counsels and defends clients in federal and state antitrust class actions and other complex litigation and in merger clearance proceedings and civil and criminal price-fixing investigations before the Justice Department and the Federal Trade Commission. His articles have appeared in the Harvard Law Review, the Yale Law Journal, and the Northwestern University Law Review.

Debbie Reynolds, the Director of EimerStahl Discovery Solutions llc, advises Fortune 500 companies on data privacy and the management of electronic evidence in high-stakes litigation. Ms. Reynolds also is an adjunct professor at Georgetown University's School of Continuing Studies, a guest lecturer for various U.S. law schools, a published author, and speaker on the impact of global data privacy in legal matters.

States. The court found that the agreement, which allowed U.S. companies to transfer the personal data of EU persons to the United States for business purposes, did not adequately protect privacy or offer adequate redress for EU individuals who opposed the processing or handling of their data by companies in the United States. In 2016, the Privacy Shield Framework replaced the Safe Harbor Framework with more robust requirements for companies and means for persons in the EU to have greater control and transparency in the handling of their data. (*See* Privacy Shield Framework Website: https://www.privacyshield.gov.)

The Safe Harbor decision and its subsequent replacement by the more rigorous Privacy Shield Framework underscore something observers have known for decades — the United States and the EU view the relationship between privacy and commerce differently. In the U.S., the privacy of personal data is based on the type of data. Our laws are more concerned with the sensitivity of the personal information in particular — such as banking information, Social Security numbers, and health information — than with a right to privacy in the abstract.

In the EU, by contrast, the privacy of personal data as an abstract matter is more broadly defined and has been upheld as a fundamental human right since the end of the Second World War. Thus, where U.S. privacy laws seek to shield sensitive information from intentional or accidental disclosure but leave businesses largely free to amass and use other user data, EU privacy laws and regulations seek to protect each individual's control over their personal information. Witness, for example, the 2014 imposition of the ''right to be forgotten'' ruling in Spain requiring Google to delete search results of EU persons upon request. (*See* Alan Travis and Charles Arthur, ''EU court backs 'right to be forgotten': Google must amend results on request'', www.theguardian.com, May 13, 2014.)

Role of Antitrust

The preeminent position afforded privacy rights in Europe has contributed to a growing divide between U.S. and EU competition authorities about the role antitrust should play in regulating the commercial use of personal information. That divide was already apparent in 2014, when Facebook, the world's dominant technology company in social networking, acquired WhatsApp, the world's most popular encrypted internet messaging application, for $19 billion.

Although both Facebook and WhatsApp are popular internet technology companies, the U.S. Federal Trade Commission (FTC) did not consider these two free consumer services to be competitors, nor did it find that the merger was likely to reduce competition between existing competitors over data privacy. It was immaterial for the FTC, from an antitrust perspective, that WhatsApp had previously marketed itself based in part on its imposition of stringent protections of user data and that a change of ownership might erode those protections.

That said, the U.S. Bureau of Consumer Protection, which is also under the control of the FTC, warned Facebook that it must adhere to the service terms expected and previously agreed upon by consumers of both technologies and must manage privacy to avoid potential harm to consumers. (*See* ''FTC Notifies Facebook, WhatsApp of Privacy Obligations in Light of Proposed Acquisition'', www.ftc.gov, April 10, 2014.)

European Commission (EC) antitrust regulators also approved the WhatsApp acquisition. But in addition to reviewing the acquisition to determine if it would harm competition, the EU antitrust regulators also considered the potential harm to consumers by the integration of EU consumer data between the two companies. Regulators were concerned that this integration could enable Facebook to compile a more fulsome dossier of personal or private information of persons in the EU than it might have otherwise been able to obtain if not for the acquisition, and that this would both damage personal privacy and give Facebook an unfair advantage over competitors. In 2017, despite its decision that the 2014 acquisition's approval should remain intact, the EC fined Facebook $122 million for not disclosing information about its technological ability to match Facebook accounts with WhatsApp accounts during the merger review process. (*See* Stephanie Bodoni, Gaspard Sebag and Aoife White, ''Facebook Fined $122 Million for Misleading EU Over WhatsApp'', www.bloomberg.com, May 17, 2017.)

Facebook's WhatsApp acquisition illustrates the central issues defining the debate over antitrust and privacy rights.

No 'Special Status' for Privacy First, U.S. antitrust authorities did not afford special status to privacy concerns but instead evaluated how the acquisition might affect competition among firms over privacy terms. Although the emergence of robust competition on privacy terms is relatively new, the framework for evaluating such competition is not. U.S. antitrust law has long recognized that businesses compete not only on price but also on the quality and terms of their offerings. Smartphone manufacturers, for instance, compete on the speed of their processors, the size of their screens, and the breadth of offerings in their app stores. Even sellers of commodities compete to improve the terms and quality of their service.

In this sense, the terms on which companies gather, protect, and use their customers' personal information are simply another non-price feature on which businesses can compete. Internet browsers may advertise that they do not track and sell browsing histories, email platforms may seek to grow their user base through promises that emails or instant messages will not be combed for advertising clues, and social networking apps may seek to assure members that their posts will be deleted rather than archived for data mining. A merger between two such companies might reduce competition among companies in that market for users and, as a result, reduce competition over privacy protections.

But U.S. antitrust law generally does not concern itself with protecting privacy rights in the abstract because it does not concern itself with promoting values other than competition. Just as antitrust authorities do not scrutinize a merger of car makers for its environmental impact, so too do they avoid evaluating a merger of social media companies for its impact on privacy. Instead, the focus is on the merger's impact on competition in the market as a whole. Regulation of substantive values remains the province of other agencies — the Environmental Protection Agency in the case of environmental concerns, for instance, or the Bureau of Consumer Protection (a division of the FTC) in the case of consumer data privacy concerns. (*See* Maureen K. Ohl-

ATRR ISSN 0003-6021

hausen & Alexander P. Okuliar, Competition, Consumer Protection, and the Right [Approach] to Privacy, 80 Antitrust L.J. 121, 151-54 (2015).

Antitrust enforcement authorities have empirical and conceptual tools for evaluating whether a merger will reduce competition on non-price terms, and it is unlikely that regulators or courts will deem those tools inadequate for assessing data-related competition. Thus, although an increase in the value of personal information likely will increase the extent to which regulators request and scrutinize how merging companies market or otherwise compete on privacy terms, companies should not expect privacy considerations to change the way mergers are evaluated.

Differences Over 'Bigness' Second, in addition to showing more concern with protecting privacy rights as a general matter, EU competition authorities also focus on the unilateral conduct of dominant firms. In the United States, antitrust law generally does not seek to prevent or punish ''bigness'' or to require companies with the market power to offer favorable terms to customers or competitors. Instead, U.S. antitrust law generally considers unilateral conduct monopolistic only if it is designed to eradicate or exclude competition through unfair or illegal means.

In the European Union, by contrast, monopolies and other large market participants can run afoul of competition authorities by abusing their dominant position to extract ''unfair'' benefits or advantages by virtue of their dominant market position. Recently, for example, the European Commission fined Google $2.7 billion for allegedly using its dominance in online searching to steer customers towards its own shopping service. (*See* Aoife White, ''Google Gets Record $2.7 Billion EU Fine for Skewing Searches'', www.bloomberg.com, June 22, 2017.)

EU competition law imposes ''special obligations'' on dominant firms, even where those firms have gained a dominant position through sheer market ingenuity. Thus, in the EU, antitrust authorities have suggested that dominant firms can abuse their leverage by offering inadequate privacy protections to consumers. One might argue that Facebook, for instance, has such a dominant position in social media that it can impose unfair privacy terms on its users, who have little choice but to accept those terms if they want access to the same social networking tool used by their friends and family. Whereas in the United States, that issue will likely be left to the market or will be regulated by consumer protection authorities, businesses should expect the EU to closely scrutinize the data-related conduct of firms with a large share of particular digital markets, such as search, networking, or online shopping.

Attention to Data Third, antitrust authorities in the EU have paid special attention to arguments that the acquisition of large amounts of data might give firms an unfair advantage over competitors. On this view, the more data a firm possesses, the more easily that firm can leverage what it knows about consumers to lock them into their product. Smaller competitors and new entrants, some believe, cannot compete because they cannot acquire or access similar stores of information. This concern might provide a rationale for blocking the merger of firms with different forms of user data, as the aggregation of data might enable the combined firm to gain an insurmountable position in the market. European Union antitrust authorities are reportedly considering changing merger regulations to place more emphasis on data aggregation concerns. (*See* Aoife White & Francine Lacqua, ''Facebook Probe Is in Antitrust, Privacy Gray Zone, EU Says'', www.bloomberg.com, Sept. 14, 2016.)

Privacy concerns might motivate regulators to place additional focus on the acquisition or conduct of firms where data privacy rights are implicated. Agency challenges to mergers are discretionary. Regulators may be more likely to decide to challenge a merger if they are concerned about the substantive or political ramifications of the deal. They also might, as with Facebook, use ancillary rules, such as penalties for failure to disclose material information, to target firms whose conduct raises data privacy concerns.

In addition, the European Union has enacted stringent privacy protections independent of its competition laws that will place significant constraints on the use of personal data. In May 2018, the penalty phase of the 2016 EU General Data Protection Regulation (GDPR) goes into effect, which has strenuous consumer safeguards that corporations located anywhere in the world that provide products and services to persons in the EU must follow. (*See* EU General Data Protection Regulation (GDPR) Portal, http://www.eugdpr.org/.)

The GDPR also has significant penalties for companies that do not comply with regulations related to the handling of the personal or private data of persons in the EU, including up to 4 percent of a company's worldwide annual revenue. The GDPR enforces the privacy rights of persons in the EU, including affirmative consent to data handling, data transparency, the right to revoke data access, data portability, and the right to be forgotten.

Businesses that provide goods or services to persons in the European Union should be prepared for more robust scrutiny of the impact of a proposed transaction on data privacy, and they should expect that scrutiny to increase as their user popularity grows. They also should explore how the EU's more stringent privacy regulations can be accommodated for European users without sacrificing the business's greater freedom of operation in the United States and other less regulated markets.

With the GDPR looming, it is not clear if EC antitrust officials will rely more heavily on the EU Data Protection Authorities (DPAs) to enforce these types of privacy rights related to handling consumer data, much like the FTC has split antitrust and consumer protection enforcement in the U.S.

It is unlikely that U.S. antitrust regulators will seek to transform competition law to enhance privacy protections. More likely, U.S. regulators will seek to protect privacy through the existing consumer protection framework.

Other Potential Issues

The market for big data is rapidly evolving. As that market grows and evolves, concerns related to user information will continue to interact with, and potentially influence, antitrust law. One area of focus for regulators, for example, may be the expanded use of the doctrine of potential competition. Although this doctrine has not yet been widely accepted by courts, U.S. antitrust authorities sometimes will argue that a merger can harm competition by eliminating a non-competitor who

either could or would enter the market if prices were to get too high. One can envision arguments that internet service markets are malleable and that a social networking provider, for instance, could easily enter the market for instant messaging, or vice versa. Adopting these arguments might place constraints on acquisitions that do not implicate direct competition.

Another concern may be price discrimination. The more data a company has about each of its customers, the easier it may be for that company to evaluate how much each customer would be willing to pay for a particular product. With enough individualized data, companies, especially monopolies, might be able to secretly charge some customers higher prices than others based on what they are perceived to be willing or able to pay. One online shopper, after all, is unlikely to see what price is being offered to another online shopper. Whether such price discrimination will occur, and whether regulators would attempt to use the antitrust laws to prevent it, remains to be seen.

ATRR ISSN 0003-6021