Antitrust Concerns About Big Data May Be Overblown

By Paul Eckles and Luke Taeschler (May 3, 2018, 1:26 PM EDT)

Arguably nothing is more in vogue in today’s economic literature than “big data.” As processing power exponentially increases and more people (and companies) join cloud-based platforms, an ever-growing amount of data is being shared across networks and devices. And this includes all types of data — shopping preferences, medical histories, career trajectories, and credit card and social security numbers.

It is hardly surprising, therefore, that the antitrust world has begun to take notice. Indeed, both the European Commission and the Federal Trade Commission have reviewed “big data” issues as part of recent investigations. And, during the writing of this article, the EC made two data-specific announcements. First, it confirmed that it is evaluating the competitive impact of agricultural-related data as part of its investigation into Bayer’s acquisition of Monsanto. Second, EC Commissioner Margrethe Vestager has gone on record that data can be “extremely valuable” (and thus potentially cause market foreclosure), statements indicating that the EC may ramp up data-specific investigations.

But the response to the big data revolution — by practitioners, academics and regulators alike — has been mixed. While one camp has called for new laws and legal theories to regulate big data usage, the other camp has cautioned against such a reactionary approach, arguing that our current antitrust tools are sufficient to handle the issues raised by the big data revolution. In fact, as the EC may begin initiating big-data-specific investigations into technology companies, United States regulators seem less likely to do so.

In this article, we offer reasons why the recent concerns about big data may be overblown and explain why the U.S. appears to be taking the better approach to big data. In doing so, we summarize the FTC’s recent statements in big data-related investigations in order to synthesize applicable antitrust principles. In sum, we argue that existing antitrust principles — when correctly applied — are sufficient to police a firm’s purported misuse of big data in the rare case where such concerns may be well-founded.

The Past: The Regulators’ Actions (and Thoughts) on Big Data

Big data has surfaced mostly in the context of the following FTC merger investigations: Reed Elsevier/ChoicePoint, Dun & Bradstreet/Quality Education and Google/DoubleClick.
Critically, because the facts and legal theories varied in each of these investigations, the agency’s decisions were likewise varied. These matters, therefore, are particularly insightful in that they demonstrate that existing legal tools are adequate to police any antitrust issues relating to big data.

**Reed Elsevier/ChoicePoint**

Both Reed Elsevier, now known as RELX Group*, and ChoicePoint offered programs to help law enforcement organizations search electronic public records (e.g., credit data, criminal records, motor vehicle records, property records, employment records, etc.). Before sharing these records with their customers, the parties first had to compile them, either by going directly to the source of the records or purchasing them from third parties. Because the two parties were admittedly the largest providers of these services (combining for over 80 percent of the market), the FTC filed a complaint to enjoin the transaction.

Critical to the FTC’s case was its allegation that existing or new players could not quickly enter the market. According to the FTC, new entry was implausible, in part, because a new player would have to “increase the breadth and depth of their public records data” as well as “improve their software and underlying analytics substantially.”[1] Speaking eight years after the 2008 deal, FTC Chairwoman Edith Ramirez explained that the key issue was that “an entrant would need analytical tools that could turn the records into services that customers would find valuable.”[2] In other words, although a new player would have equal access to the underlying data, the new player still would lack the technical and analytical ability to turn the data into a useful product. Thus, the FTC’s concern was not about the inability to procure the data but rather the inability to effectively manipulate it.

To settle the case, the parties agreed to divest to Thomson Reuters the ChoicePoint assets related to electronic public records services; ChoicePoint also agreed to a transition services agreement, through which it would help Thomson Reuters understand the underlying algorithms and analytics required to operate its programs.

**Dun & Bradstreet/Quality Education Data**

At issue in the Dun & Bradstreet/Quality Education Data merger was educational marketing data for K-12 students. The relevant data — contact, demographic and other information about K-12 educators, administrators and school districts — was sold by the parties to third-party businesses, who in turn used the data to create products and services for K-12 educators and administrators. Together, Quality Education Data and Dun & Bradstreet owned 90 percent of the business in the space.

As in Reed Elsevier/ChoicePoint, the FTC found new entry unlikely, but this time for a different reason. Unlike in Reed Elsevier/ChoicePoint — where the issue was that a new entrant could not manipulate the relevant data — the issue in Dun & Bradstreet was that the new entrant could not readily assemble the relevant K-12 data. Indeed, the FTC alleged that a new entrant could not develop “an up-to-date database with the size, breadth and scope of market coverage comparable, at a minimum, to that held by QED.”[3] (The FTC also argued that, even if a firm could assemble the requisite database, it still would have difficulty competing because it lacked brand awareness, which would take years to build.){[4]} And Ramirez confirmed as much in her 2016 speech, stressing that the Dun & Bradstreet/Quality Education data set had “unique characteristics,” such that customers did not consider other data sets as viable competitors.[5]

To settle the case, the parties agreed to divest an updated and augmented K-12 database to Mailings Clearing House, a fringe competitor that could effectively use the data set.[6] (The parties also agreed to divest the QED brand and associated intellectual property to assuage the FTC’s aforementioned "brand awareness" concern.)
Unlike the first two mergers, the Google/DoubleClick merger differed in a critical respect: The FTC declined to file a complaint to block the deal and, instead, closed its investigation and allowed the transaction to close as-is. Although there were a variety of antitrust issues and legal theories discussed in the FTC’s decision closing the investigation, here we focus only on two: (1) the idea that the deal may cause anti-competitive effects by giving Google an overwhelming amount of consumer data, and (2) the idea that the deal would result in decreased privacy protection for consumers.

Beginning with the FTC’s competitive effects analysis, the FTC found that Google’s acquiring of DoubleClick’s data would not enable Google to exercise market power for three main reasons. First, much of the customer data in DoubleClick’s possession actually belonged to web publishers (not DoubleClick), and the contracts between those publishers and DoubleClick prohibited disclosure of the data. Because Google agreed to honor those contractual provisions, it would be unable to use the data with third parties in a way that would be anti-competitive. Second, even if Google could utilize DoubleClick’s customer data, that still would not cause competitive concerns because the data did not “constitute an essential input to a successful online advertising product.”[7] As the FTC explained, most of Google’s competitors likewise possessed their own valuable stores of data; the FTC identified Microsoft, Yahoo and Time Warner as specific examples of companies with their own data sets. Because other players had access to their own useful data, and because nothing about DoubleClick’s data was particularly unique, the FTC saw no competitive concerns with Google acquiring DoubleClick’s databases of customer information.[8]

The FTC also refused to block the merger based on privacy-related concerns alone. In fact, the FTC explained that it had no legal authority to block the deal on strictly privacy grounds, and that doing so could “pose a serious detriment to competition,” particularly in such a nascent industry.[9] The FTC did acknowledge, however, that it investigated whether the deal would impact nonprice attributes of competition — like consumer privacy — but had found no evidence that would be the case.[10]

The Future: What Have We Learned?

Looking at the FTC’s history with big data illuminates a few principles. Specifically, we can understand the situations in which big data concerns may be legitimate (and thus trigger
regulatory action) as well as the situations in which big data does not pose serious concerns. Based on the FTC’s past precedent, big data may be an important issue in the following circumstances.

- **When Data — or the Requisite Tool to Use the Data — Is Unique:** Regulators may take interest in big data usage when the data in question (or the tools required to use the data) are sufficiently unique, such that another firm cannot replicate the data set or the tools required to use it.

- **When Data Is an Essential Input:** Regulators may take interest in cases where data sets are viewed as “essential” inputs required to create downstream products.

Importantly, in these types of cases, regulators can use — and in some instances already have used — existing antitrust jurisprudence to bring merger challenges. Indeed, the antitrust laws allow regulators to bring challenges when (1) a product is relatively unique and high barriers to entry prevent new competitors from entering the marketplace, and (2) inability to access an essential input would foreclose a substantial share of the market. And nothing in the antitrust laws — or applicable case law — prevents regulators from doing so when data itself is the alleged entry barrier or essential input at issue. Indeed, as Nigro explained in his December 2017 remarks: “Existing antitrust tools have been adequate to address these issues in the past, and they are adequate now too.”[15]

Although this article has discussed big data in the context of merger enforcement decisions, the same principles should apply to conduct-based enforcement actions, particularly in Section 2 cases. Just last month, Assistant Attorney General Makan Delrahim explicitly said as much, explaining that regulators must be careful bringing Section 2 enforcement actions so they do not “kill the golden goose of innovation.”[16] Delrahim advised regulators to bring only “evidence-based” challenges, and questioned some commentators’ calls to expand the predatory pricing doctrine such that it would be easier to challenge conduct by technology companies that operate digital platforms.[17]

In sum, the reaction over “big data” — and the resulting calls for increased enforcement efforts — appear to be overblown at best and empirically unfounded at worst. As recognized by economists Anja Lambrecht and Catherine E. Tucker, a firm’s possession of “big data” will rarely on its own confer an unfair competitive advantage, much less create serious barriers to entry.[18] And this is true for a variety of reasons. Sometimes data grows stale quickly, such that a firm’s possession of a specific data set conveys no long-term advantage — e.g., a consumer’s browsing history reflecting a desire to purchase golf clubs is not as useful for advertisers once the consumer has purchased the clubs. In other instances, different data sets can be used for the same or similar purposes — e.g., movies that consumers “like” on Facebook may overlap with movies consumers watch on Netflix or see in theaters through MoviePass subscriptions. In short, not only is it rare for big data use to cause anti-competitive concerns, but there are also existing (and sufficient) tools for regulators to deploy in the rare case where data concerns are warranted.

---

Paul M. Eckles is a partner and Luke T. Taeschler is an associate in the New York office of Skadden Arps Slate Meagher & Flom LLP.

*Law360 is owned by LexisNexis Legal & Professional, a RELX Group company.*

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be
taken as legal advice.


[4] Id.


[8] Id.

[9] Id. at 2.

[10] Id. at 2-3.


[17] Id. at 5.