BIG DATA: INTERACTION BETWEEN DATA PROTECTION RULES AND COMPETITION LAW AND THE IMPLICATIONS FOR RETAILERS

Let me briefly introduced myself. My name is Panayiotis Agisilaou and I am the managing director of Trojan Economics, a consultancy company specializing in competition economics. I am also a visiting lecturer at the Open University of Cyprus.

I am delighted to be here today to talk to you about “Big data, the interaction between data protection rules and competition law and the implications for retailers”.

INTRODUCTION

Data collection and data mining is not a new phenomenon. Those working in the commercial sector have been collecting and combing large data sets to improve segmentation of products to customers and better understand the market in which they participate for a long time.

However, the rapid technological progress, induced to a large extent by the digitization of markets and the economy more generally, have drastically increased the possibilities to collect, store and process data. Over the last few years, the economic value of data has exponentially increased so that today data is considered a driver of growth and innovation, and a source of power. According to a recent article by the Economist, data is now the most valuable resource in the world, beating out oil.
Before I point out the benefits of commercial exploitation of data for firms and the potential harmful effects on competition and consumers' welfare, I would like to provide a definition for “big data”.

Big data can be defined as a large volume of data that has the potential to be mined for information and used in machine learning projects and other advanced analytics applications. Big data is often described by 5 characteristics, known as the 5 “V”s; Volume, Velocity, Variety, Veracity, and Value.

- **Volume** refers to the large volume of information produced every second.
- **Velocity** refers to the speed of data creation, processing, and analysis.
- **Variety** refers to the different types of information that a data set may contain and the different sources of data.
- **Veracity** refers to the quality of data and their reliability in terms of accuracy.
- **Value** refers to the economic value of data for firms, in particular for devising business strategies and business models and making strategic decisions.
PRO-COMPETITIVE EFFECTS

Now, I would like to talk about the potential benefits of big data for firms.

• First, big data can help firms to better understand consumers’ preferences and their response to price changes. This enables the implementation of targeted marketing strategies (e.g., targeted advertising and promotions), which increase firms’ sales and profitability.

• Second, big data allows firms to offer personalized products that are better aligned to consumers’ needs. For example, retail firms can offer personalized suggestions/recommendations to their customers for products based on data regarding their purchasing history or data from transactions with other customers which share similar profile characteristics.

• Three, the analysis of big data often results in valuable inferences regarding the development of new products/services or the improvement of existing products/services through learning effects. For example, a firm can identify gaps in the market or areas where there is excess demand. Big data also enable firms to rectify faults/errors based on their customers’ feedback or improve their pricing or other algorithms.

• Four, big data can enhance firms’ operational effectiveness. For example, big data analytics can help firms to better understand trends in demand, so that to promptly adapt their production and inventory. Another example involves the simplification and acceleration of transactions with customers based on their data from
previous transactions with the firm (such as delivery address, payment method, card details).

- Five, the most pervasive benefit resulting from big data is the ability of firms (especially those operating in multisided markets) to offer services in exchange for their customers’/users’ data. Firms subsequently use the data collected to offer targeted advertising services which finance the services provided to consumers without monetary compensation. Prominent examples of services which are based on this business model are email accounts, the social media, applications on mobile devices and internet search engines.
POTENTIAL CONCERNS

Although the collection, processing and commercial use of big data produces significant benefits, there are some features of big data which when combined with specific structural market characteristics and the nature of the competitive process, may cause harmful effects on consumers’ welfare. For example, if the data set of a firm is unique and cannot be reproduced then big data can be a source of market power.

Moreover, by collecting more data, an established firm has more scope to improve its products, either by learning or experience effects or by investments in R&D which are financed by the revenues generated from the commercial exploitation of the accumulated data. As a result, an established firm may attract more customers, generating even more data, a process which triggers network effects (i.e., the more customers a firm has, the more attractive its product/service become, due to quality improvements that result from the access to more data). As the data gap, and, consequently, the product/services quality gap, between the dominant firm and smaller rival firms widens, the intensity of the competitive pressure a dominant firm encounters, in terms of quality and innovation, diminishes. Under these conditions, the market may lead to a winner-takes-all result where high concentration (even monopoly) is the most likely market structure outcome.

Before I present the most notable data-driven theories of competitive harm, I would like to highlight that the accumulation or control of big data does not in itself constitute an infringement of Competition Law (Competition Law refers to a set of laws and regulations aiming to preserve a level playing field in markets by prohibiting unilateral or coordinated anticompetitive behavior by firms). What matters for
Competition Law enforcement is the conduct of firms, and in particular, whether a firm in a dominant position uses its data as a tool to exclude its competitors from the market or to exploit locked-in customers. Moreover, Competition Law enforcement has a critical role in cases where firms conspire to suppress competition by coordinating their strategic decisions (such as prices).
**DATA-DRIVEN THEORIES OF HARM**

Recent academic literature and policy studies have identified several data-driven theories of competitive harm. In particular, harm related to refusal to access to data, price discrimination, tying, algorithmic collusion and reduction in privacy protection.

I will now expand on these theories.

**REFUSAL TO ACCESS TO DATA**

The first theory of harm is related to the refusal on behalf of a dominant firm to provide access to its data without objective justification.

In particular, if the dominant firm owns a data set which is truly unique or its reproduction entails a prohibitively high cost, then a refusal to provide access to its data is likely to distort competition, as long as the dataset is essential to the activity of the firms requesting for access.

Moreover, refusal of access to data could also be deemed anti-competitive if it is discriminatory. For example, when a dominant firm refuses to sell its database to certain customers but would sell it to other customers.

Discretionary access to strategic data by a vertically integrated dominant firm may also distort competition. A good example of this is when a dominant firm which operates a platform such as an online market place and at the same time operates as an online retailer obtains privileged access to information about other retailers which sell on its market place. By exploiting this information, the integrated platform could gain an unfair competitive advantage in the retail sector since it will be in a better position to adjust the range and the prices of its products. I mentioned this example since the European Commission is currently investigating allegations that
Amazon uses data from third-party transactions generated via its Marketplace to enhance its own online retail offering.

EXCLUSIVE CONTRACTS

There are also other ways in which dominant firms may increase the barriers to entry or foreclose potential competition. In particular, dominant firms may pursue to maintain their data-related competitive advantages by gathering large amounts of data through exclusive agreements with third-party providers of data (i.e., exclusive licensing or exclusive access to an important data set). These agreements essentially prevent third-party providers from doing business or sharing the same or similar data with anyone else other than the dominant firm.

An example of how exclusive agreements can evolve in a data-related situation is the Google AdSense case which the European Commission is currently investigating. In short, the European Commission claims that Google’s agreements with the websites on which its AdSense ads are displayed are anticompetitive since Google requires exclusivity from participating sites, preventing them from displaying ads from rival advertising networks.
PRICE DISCRIMINATION

The second theory of harm is related to price discrimination. Price discrimination occurs when different consumers are charged different prices for the same product.

In a data-related situation, a dominant firm can set different prices for the different customer groups it has identified thanks to the data collected about their maximum willingness to pay.

While consumers can theoretically choose to shop elsewhere to escape unfavorable price discrimination, switching to rivals’ products/services will depend on the level of search cost and switching cost. When those costs are relatively high, then the negative effects of price discrimination on consumers’ welfare are more profound. Consumers’ naivety (due to behavioral biases, such as, inertia or ignorance) also tend to amplify the detrimental effects of price discrimination.
TYING

The third theory of harm is related to tying. Tying refers to the commercial practice of selling a product to a buyer only if the buyer also agrees to purchase another product from the same seller.

A data-related example of tying is the situation where a dominant firm that owns a highly valuable dataset makes an arrangement under which it provides access to its dataset on the condition that the buyer also purchases its data analytics services. With this practice, the dominant firm essentially attempts to leverage its market power to other contestable markets or maintain its market power by preventing its competitors to obtain a critical mass of customers.

A recent example of tying in a big data context is the Google Android case. In that case, the European Commission ruled that the practice of Google to restrict Android device manufacturers and mobile operators to pre-install Google Play Store without having to install Google Search app and Google Chrome Browser led to a ‘status quo bias’. To put it more simply, users were more likely to stick to apps that were pre-installed on their devices than to switch to apps that still had to be downloaded. As a consequence, rival search engines were prevented from collecting valuable user data, allowing Google to cement its dominance as a search engine.
ALGORITHMIC COLLUSION

The fourth theory of harm is related to the increased market transparency (especially in online retail markets) which tends to facilitate collusive behavior. In particular, due to big data firms may have more access to their competitors’ prices which makes it easier for them to agree on a common price by avoiding costly experimentation in the market. Moreover, the increased market transparency due to big data enhances the sustainability of collusion, since the detection of cheating and retaliation of defections becomes easier / faster (e.g., real-time).

I would like to draw your attention to the final report of the European Commission regarding the E-commerce sector inquiry (May, 2017), according to which 53% of the responding retailers confirmed that they track online their competitors’ prices, 67% of them by using software, while 78% of them claimed to subsequently adjust their prices.

Firms can also use big data to fix prices by means of sophisticated algorithms. For example, the ability to quickly analyze large amounts of data by means of algorithms makes it easier to coordinate and monitor the behavior of a large number of firms. Therefore, collusion becomes possible in less highly concentrated markets.

Furthermore, firms can use sophisticated mechanical learning and artificial intelligence to implement a collusive agreement by integrating into their price-setting algorithms their competitors’ reactions to price changes and adjustments to the respective market conditions.

A recent example of algorithmic collusion involved certain poster retailers on Amazon Marketplace. These retailers had initially agreed to avoid underbidding each other. Subsequently, when they realize that manual
price adjustments are too complex and time-consuming, they decided to use a repricing software which equalized the prices of the colluding retailers as long as no third-party dealer had offered a lower price.
A question that has gained great attention recently is whether competition analysis should consider data protection and privacy concerns.

At first glance, it can be held that privacy concerns are not in themselves within the general scope of Competition Law. This would seem to be consistent with a landmark decision of the Court of Justice of the European Union in 2006 (Asnef-Equifax) where it was held that any possible issues relating to the sensitivity of personal data are not, as such, a matter of competition law, they may be resolved on the basis of the relevant provisions governing data protection.

However, privacy issues can play an important role in competitive dynamics, whenever data protection or the transparency of data protection policies of firms constitute key parameters of non-price competition (as an illustration consider Duck Duck Go search engine which claims not to collect or share any personal information). More specifically, data protection and privacy standards can be considered to be parts of the ‘quality’ parameter of a service. Therefore, a reduction in the level of privacy protection implies a reduction in the quality of the service itself. This argument was recently acknowledged (2016) by the European Commission when examining the acquisition of LinkedIn by Microsoft.

A dominant firm may also exploit consumers by imposing unfair terms and conditions with respect to the collection of customers’ data from third parties or demand excessive data from its customers.
An example of the enforcement of Competition Law to data collection and privacy issues is the recent decision of the Federal Cartel Office in Germany against Facebook for abuse of its dominant position among social networks. In particular, it was held that Facebook abused its market power by collecting data from various other Facebook-owned services such as WhatsApp and Instagram or from third-parties which they were using Facebooks’ analytics services or the “Like button”, and by combining that data with a user’s main Facebook account. According to the decision, Facebook can collect data from other sources but it cannot combine that data with a user’s main Facebook account unless users give their explicit voluntary consent. Moreover, users who decline to provide their consent should not lose access to Facebook’s services.
FINAL REMARKS

In conclusion, let me sum up my main points.

Big data can have a concrete impact on competition. On the one hand, they can stimulate innovation, enhance operational efficiency and help improve products/services quality. On the other hand, they can be a source of market power, trigger abusive behavior and enhance incentives to engage in anticompetitive collusion.

Competition Law enforcement on big data-related issues is more likely when the protection of private data or the transparency of data protection policies or the fairness of the terms and conditions underpinning the collection of data, constitute key parameters of non-price competition and thus affect competitive dynamics.

Thank you all for listening; it was a pleasure being here today.