Report of workshop on Privacy, Consumers, Competition and Big Data 2 June

On 2 June 2014 in the European Parliament in Brussels, the European Data Protection Supervisor hosted a workshop on the policy implications for the fields of data protection, competition and consumer protection of the rapidly expanding digital economy in the EU and in other regions, particularly the U.S. The event followed the publication, as part of the EDPS' advisory and consultative role, of the Preliminary Opinion on the subject.[*]

Discussions took place in a frank and collaborative spirit under the Chatham House Rule, and explored technological advances and market for 'big data' analytics, and the unique set of challenges posed for competitiveness, choice, consumer welfare and privacy. They involved around 70 experts from European regulators, plus the US Federal Trade Commission, academia, think tanks and legal practice.

This report of the workshop is structured according to the five big, overlapping themes which were subject of discussions:

1. The features of the digital economy and the importance of personal data to its development
2. The aims of competition law and how those are played out in practice
3. The various ways in which the interests of the 'consumer' are understood in competition law and consumer protection law
4. The extent to which privacy is considered a competitive advantage in digital markets
5. Challenges for enforcement cooperation in the fields of competition, consumer protection and data protection

At the end of this report is a series of questions grouped around these themes which merit further investigation. Anyone interested in more information on this project or to contribute views and expertise is welcome to contact us at edps@edps.europa.eu

1. Personal data in the digital economy

The digital economy has seen rapid change and consolidation as a result of factors such as network effects, the biggest players' vertical integration and establishment of proprietary standards.

According to the OECD, 'big data related' mergers and acquisitions rose from 55 in 2008 to 134 in 2012. The internet sector is hugely successful with revenue per employee in 2011, among the top 250 companies, of over $900 - over twice as high as for the ICT industry overall (OECD). Internet companies could enjoy 'economies of scope', network effects of more data attracting more users attracting more data, culminating in winner-takes-all markets and near monopolies which enjoy increasing returns of scale due to the absolute 'permanence' of their digital assets.

[*] Preliminary Opinion of the European Data Protection Supervisor: Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014.

The U.S. and the EU had a common experience of these dynamic markets. These markets encouraged use of two-sided platforms: one side involved 'attracting eyeballs', collecting data and extracting value using algorithms; the other side sold services. The data collection side of this platform was prone to network effects, and assertion of IP rights and protection of trade secrets to guard against ease of entry to the market, innovation cycles and creative destruction.

Data have been described as a 'non-rivalrous' good in that they can be used for multiple purposes on multiple occasions without reducing their value for other users. Data are unlike other economic goods in that their value depends on the means of combining them and extracting knowledge from them. An initial question is therefore to define relevant data markets with reference to how personal data is used.

Economic actors in the digital industry have been termed 'prosumers' who produce as well as consume information; individuals leave permanent traces across cyberspace, like silkworms depositing 'silk' which is then 'farmed' for different purposes by public and private organisations.

The internet can be understood as a 'networked physical system'. Individuals usually do not know about, or have not agreed to, personal data processing by companies, not only in services like social media, but also in liberalised markets such as energy and telecoms. The consumer may – irrationally - spend more in the current agreement than if he/she went to a feasible alternative, while the trader remains opportunistic. You do not need to pay cash for there to be a transaction. For zero cost services – like social media, search and gaming - the competition authorities' 'SSNIP' test (i.e. small but significant non-transitory increase in price which estimates products to which customers would switch in the case of a 5% or 10% price increase) could not be applied. The real cost of the transaction is different than the price: it includes the price plus anything else parties consider of value.

The result can be growing information asymmetry between service provider and user, especially where a firm becomes dominant through control of masses of personal data which may then be processed by third parties without the data subject's knowledge. Businesses seek to develop more realistic and detailed user profiles and use control of that data to expand into new markets. Transaction cost economics and behavioural economics indicate that these markets are inefficient due to this informational asymmetry, while competition fades away when bilateral dependence is established between consumer and trader.

In competition law, there have recently been digital market cases in which the intangible asset of data was considered in the analysis (see for example Commission decisions on merger cases M.7023 Omnicom/Publicis case and M.5727 Microsoft/Yahoo case).

2. Aims and application of competition law

Absent any prescribed 'unifying objective' for competition law in the Treaties, there has been much debate over potential aims like efficiency, market integration and consumer welfare. The European Commission has taken an economic effects based approach, while the CJEU has not endorsed any single objective. Competition enforcement can de-concentrate markets in order to facilitate more choice and more informed choice. This is not a precise science, and basic concepts can and should be interpreted flexibly in order to understand properly market dynamics.

EU authorities consider each specific case on its own merits. Where there is a recurring issue, the Commission may consider issuing guidance after issuing decisions on cases first. The question was posed as to whether a retrospective or ex-post evaluation of certain merger or antitrust cases could provide insights into the real impact of decisions on the market, including choice and quality.

EU competition law sanctions certain, very specific forms of private conduct that are detrimental to competitiveness. Its analysis referred to the 'parameters' of competition, namely price, output, product quality, product variety (i.e. choice) and innovation.[†]

Merger cases are ex-ante investigations which rely on forecasts of the effect of the merged entity on the market. For services offered at price zero, one challenge was measuring the probability of the merged entity increasing the price. The turnover thresholds which apply in merger cases also might not be suited to 'big data' markets and where personal data are a crucial input and asset.

For antitrust cases (i.e. ex-post investigations) under Article 102 TFEU, the concept of 'essential facility' was much contested, and it was very difficult to establish whether personal data held by a dominant company is erected as a barrier to entry by competitors.

Some argued forcefully for integrating competition on privacy into enforcement procedures, and assessing to what extent a merger of two companies competing for the same data would foreclose competition or affect the transparency of privacy policies and motivation to invest in privacy enhancing technologies.

The CJEU in its 2013 *Allianz Hungaria* judgment [Case C-32/11] recognised that an infringement of one area of law could possibly be a factor in deciding that there has been an infringement of competition law as well, therefore it was possible that a breach of data protection law could constitute an infringement of competition law (e.g. through exclusionary behaviour or collusion) as well.

However, the CJEU has also been clear in a judgment on exchange of personal information on solvency and credit worthiness, 'any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, [as] they may be resolved on the basis of the relevant provisions governing data protection.' [Case C-238/05, *Asnef-Equifax*, paragraph 63].

In any case, competition policy must nevertheless be vigilant in case dominant companies use personal data to gain further advantage over their competitors. Competition authorities said that such abusive behaviour had not yet been uncovered.

Some speculated decisions in competition cases might have been different had they been taken after the entry into force of the Lisbon Treaty, under which EU has a positive obligation to uphold fundamental rights, and not simply a negative obligation to avoid abuse. These fundamental rights include not only privacy or data protection but also the freedom to establish a business and freedom of expression. Competition law and merger control were explicitly used to ensure media plurality, a goal closely tied to the right to freedom of expression; it is open to debate whether the time is approaching where plurality of choice in privacy-intrusive, personal data-fuelled digital markets should be given similar treatment.

[†] Commission Guidelines on the application of Article 81(3) of the Treaty (2004/C 101/08).

3. Consumer interests, consumer welfare

Consumer welfare is emerging as a standard, as seen in the Guidance Paper on enforcement priorities in applying Articles 101 (3) and 102 (although, as discussed above, this standards has not been endorsed by the CJEU). The Court has referred to consumer interest in free competition (*Zuchner* C-172/80 [1981], *Cooperatieve vereiniging Suiker UA Cases* 40-48,50,54-56,111, 113 and 114/73 [1975], RTE and ITP [1995] C-241/9 P, C-242/91 P), and consumer welfare is a consideration which could address deceptive practices (Astra Zeneca ECJ) in privacy policies. But the Court has also stated in its 2009 judgment in *Cases C-501/06P, C-515/06P and C-519/06P, GlaxoSmithKline* that 'there is nothing in Article 101(1) to indicate that agreements must deprive consumers of certain advantages in order to have an anti-competitive effect... Article 101 TFEU aims to protect not only the interests of competitors or of consumers, but also the structure of the market.'

Choice is a core parameter in competition analysis. On the one hand, to what extent can a consumer freely consent to action by a dominant undertaking, whether it is price increases or unfair or deceptive amendments to privacy policies? On the other hand, to establish abuse of dominance it must be proven that the undertaking has foreclosed firms from the market or exploited the consumer. At present, there is a scarcity of case law on consumer exploitation.

There is some support for the notion of consumer sovereignty in competition law, but this risked punishing dominance itself. It could also introduce goals which are not within the competence of competition authorities; data protection should not be used to structure markets.

Recently there appears to be a blurring of line between consumer protection and competition. Such a trend would accord with the Article 12 TFEU requirement for 'consumer protection requirements to be taken into account in defining and implementing other Union policies and activities', and the description in Article 102 of abuse of a dominant position which may include 'limiting production, markets or technical development to the prejudice of consumers. Overall, however, insofar as consumer welfare is the ultimate goal, competition authorities still tend to view this aim through one particular microeconomic perspective leaving other dimensions of consumer welfare to other specialised authorities.

4. Privacy as a competitive advantage

Data protection rules in the EU are not intended to choke creativity but rather to provide a condition for success and competitiveness.

There were plenty of examples of start-ups who seek competitive advantage through their privacy policies. But the market for privacy enhancing technologies is weak, as attested by the very low number of patents for 'PETs' compared to those granted for data analytics. Data are increasingly profiled in silos from which the user often cannot opt out. In effect, it has been argued, social networks already themselves regulate user privacy, and dictate which code can be used by third parties.

Data portability could be a positive force for privacy as well as competitiveness, but it remained unclear how it could work in practice and whether it could be effective without dominant networks being compelled to interconnect. Users would need to know what data is held about them and for what purpose. They would also need to be able to retrieve 'dead data' lurking in defunct 'zombie'

accounts of former users of existing networks, or zombie networks which were once popular but have since been driven from the market. Others argued however that the duty to deal or to supply, applied at the same time as the right to data portability, could have the effect of *dissuading* investment in privacy-enhancing technologies.

More transparency on privacy policies was essential to enable informed choice, using for example simple graphics, pictures or icons to explain how, by whom and under whose responsibility personal data would be processed. Greater consumer trust could improve the quality and accuracy of data which would in turn benefit businesses.

5. Enforcement in practice

Various fora for cooperation within the EU and internationally exist. Some authorities have formed joint investigations such as CNIL and French consumer authority on IP tracking/ dynamic proxying. The Commission, like several national authorities, is a single entity although also a composite of separate responsibilities carried out on distinct legal bases.

The various separate enforcement bodies operate against a background of different cultures and powers. Data protection authorities have varying and still relatively modest power to apply sanctions, for example, but on the other hand their constitutional independence is entrenched in the Charter of Fundamental Rights. Consumer protection authorities have widely varying enforcement powers across the Member States, are often under-resourced, and are required to 'patrol the gaps' where sectoral authorities (e.g. for telecommunications) do not regulate.

Where large retailers, social platforms and telecoms collect vast amount of personal data which are often aggregated by other firms, there is a clear risk of abuse. This will normally fall within the reach of data protection and consumer protection enforcement. Therefore, consumer protection and data protection authorities have a common interest in helping the individual realise the value of their own data. For consumer protection and data protection authorities, however, it is challenge enough for them to work together within existing cooperation structures.

Enforcement regimes should not be 'instrumentalised' to achieve the aims of the other regimes. The purpose was not for authorities to encroach on each other’s areas, but rather to talk and to cooperate where there was an overlap of aims and focal points. But the question is who can take the initiative in relation to regulating the digital economy, as the Commission has itself done for the food and pharmaceutical industries. It is not unreasonable to expect authorities to take a holistic decision, balancing all interests.

Overall, this issue concerns the extent to which the problem is lack of dialogue, uneven enforcement powers and power to impose effective remedies.

Conclusions

It was agreed that stakeholders, regulators and experts should continue to talk about how data protection principles, in particular those of purpose limitation and legitimate interest, can be applied to the digital economy, and how the various policy areas could be deployed most effectively to facilitate transparency, choice and competitiveness in privacy policies which protected the fundamental rights and interests of individuals. Data protection and competition specialists do not necessarily speak the same language. Laws may currently be applied effectively to address visible

large scale abuses. But the laws seem not to cover the incremental ‘day-by-day drops into the ocean of data’ which are assembled to construct user profiles, where even seemingly innocuous data can reveal sensitive information. This process will be accelerated as more and more devices go online, which will in turn intensify the need for privacy by design, high standards of data security and data minimisation.

This event has generated momentum for discussing these issues. Now that 'the genie is out of the bottle,' the EDPS would be pleased to continue to act as a conduit for ideas and further discussion. Five themes in particular are suggested below.

Suggestions for further discussion

1. Understanding the value of personal data

Data are not like other economic goods – they have value only if accompanied by a means of extracting knowledge. How can the value of personal data be assessed as a currency and an asset in competition analysis? To what extent is ‘big data’ composed of personal data?

2. Reviewing approaches to market analysis where personal data are an asset

The traditional tools of competition analysis are flexible but, according to some, produce strange outcomes in the context of the digital economy. Arguing that data protection should be 'an additional factor' in competition enforcement is unlikely to gain much support. Instead, how can we apply the 'parameters of competition’ - especially price, quality and choice - in explaining the impact on privacy and data protection?

3. Competition law enforcement: wider issues

Is it right for competition authorities just to look at one case at a time? Is there a case for a wider study, guidelines etc. to inform authorities dealing with antitrust and merger cases in the digital economy? One recommendation was to carry out retrospective/ ex post analysis of the impact of competition decisions. Another suggestion was that the Lisbon Treaty has created a positive obligation on the competition authorities including the Commission to uphold fundamental rights, and that privacy protection merited similar attention as the preservation of media plurality.

4. Weak markets for privacy enhancing services

There was general agreement that privacy was rarely viewed as a competitive advantage while there were few applications for patents for privacy enhancing technologies compared to, say, data analytics. Data portability could be a positive force for privacy and competitiveness but how could it work in practice?

5. Cooperation between authorities

The capability and willingness of supervisory authorities to cooperate are central to a more holistic approach. It appears that especially consumer authorities lack enforcement powers, while cooperation between authorities is often talked about but rarely occurs in evidence. What practical steps could be taken to address this, for example joint investigations or guidance?

EDPS, 11 July 2014