EUROPEAN DATA PROTECTION SUPERVISOR

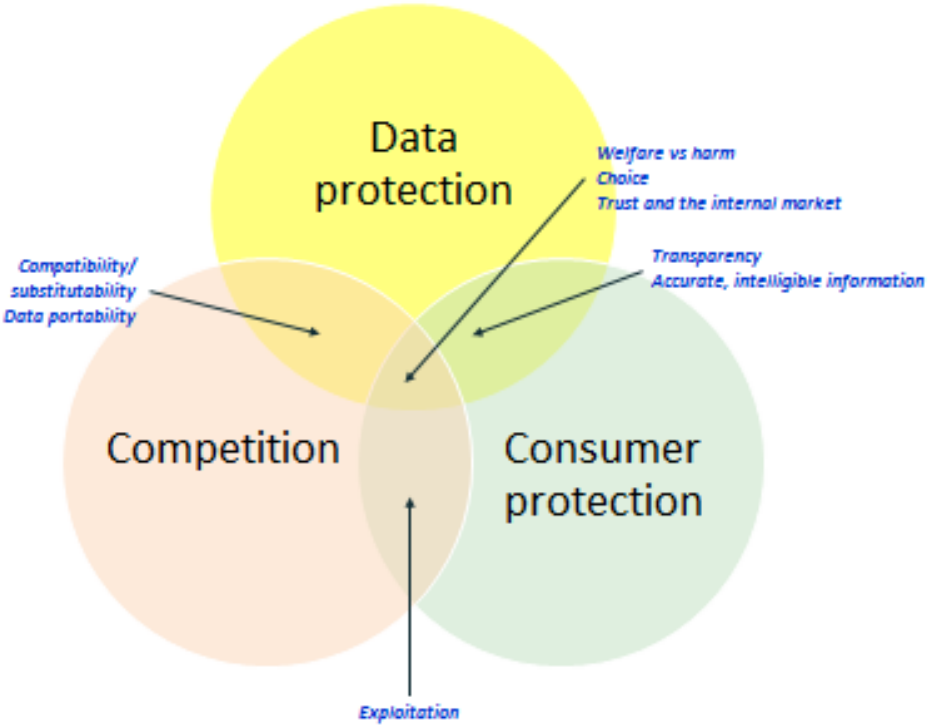
*Preliminary Opinion of the European Data Protection Supervisor*

# 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

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel: 02-283 19 00 - Fax: 02-283 19 50


Data protection
Welfare vs harm
Choice
Trust and the internal market
Compatibility/ substitutability
Data portability
Transparency
Accurate, intelligible information
Competition
Consumer protection
Exploitation

*Summary*

EU approaches to data protection, competition and consumer protection share common goals, including the promotion of growth, innovation and the welfare of individual consumers. In practice, however, collaboration between policy-makers in these respective fields is limited.

Online services are driving the huge growth in the digital economy. Many of those services are marketed as 'free' but in effect require payment in the form of personal information from customers. An investigation into the costs and benefits of these exchanges for both consumers and businesses is now overdue.

Closer dialogue between regulators and experts across policy boundaries can not only aid enforcement of rules on competition and consumer protection, but also stimulate the market for privacy-enhancing services.

**Contents**

*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

## 1. Introduction

1. The digital economy holds many advantages for consumers and citizens. Online services offer unprecedented scope for social connections, innovation and efficient problem-solving. At the same time, users of these services disclose masses of information about themselves. The volume and variety of data generated cannot be handled by traditional data mining and analysis technologies, but control of this information is now increasingly possible thanks to the development known as 'big data'.[1] Extracting value from big data has become a significant source of power for the biggest players in internet markets. Not all big data is personal, but for many online offerings which are presented or perceived as being 'free', personal information operates as a sort of indispensable currency used to pay for those services. As well as benefits, therefore, these growing markets pose specific risks to consumer welfare and to the rights to privacy and data protection.

2. EU principles and rules on data protection, competition and consumer protection have been designed to promote a thriving internal market and to protect the individual. Greater convergence in the application of these policies could help meet the challenges posed by the big data economy. However, to date, policies have tended to develop in parallel with little interaction on subjects of common concern.[2] Moreover,

[1] Big data 'refers to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed using computer algorithms'; Article 29 Working Party, Opinion 03/2013 on purpose limitation, p. 35. According to an alternative definition, big data means 'datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyse'; McKinsey Global Institute, 'Big data: The next frontier for innovation, competition, and productivity', June 2011. In this preliminary Opinion 'big data' is used as shorthand for the combination of massive personal data collection and analytics on high variety, high volume datasets.

[2] This preliminary Opinion develops the themes outlined by the EDPS at a seminar in Brussels on 13 June 2013 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-06-13_Speech_CB_Brussels_EN.pdf'. Related discussions took place in 2010 at the 32nd International Conference of Data Protection and Privacy Commissioners in Jerusalem. Moreover, Commission Vice-President Joaquin Almunia gave a speech on 'Competition and privacy in markets of data' in November 2012 (http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm). In February 2013 at the New Frontiers of Antitrust 4th International Concurrences Conference, following a roundtable discussion on the subject 'Personal data: Will competition law collide with privacy?', the Commission Director General for Justice called for greater consideration to be given to the interaction between data protection and competition law; Françoise Le Bail entitled 'Protection de la vie privée et des données personnelles: l'Europe à l'avant garde', Concurrences Revue des droits de la concurrence: Competition Law Journal : Demain la concurrence New Frontiers of Antitrust Colloque l Concurrences, N° 2-2013. A similar debate in the United States has been ongoing in particular since the Federal Trade Commission decision on the Google DoubleClick merger (see footnote 76) and the dissenting opinion of then Commissioner Jones Harbour http://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf; for an update on Ms Harbour's analysis see her essay 'The

EU policy makers and regulators have until now typically focused on markets for products and services traded in exchange for money. As consumers and businesses both adapt to and propel constant changes in technology, there is an onus on policymakers and regulators to keep pace, as reflected in the recent political commitment to the 'completion' of the 'Digital Single Market'.[3]

3. The EDPS promotes a 'data protection culture' in EU institutions and bodies where data protection principles find expression in all relevant areas of policy and law.[4] As a contribution to that aim, this preliminary Opinion seeks to stimulate a dialogue between experts and practitioners, including EU institutions and national regulatory authorities from the competition, consumer protection and data protection fields. The EDPS will then reflect on the views and ideas arising from this exercise in a follow-up Opinion and include recommendations for action.

4. Chapter 2 of this Opinion begins by outlining trends in the digital economy and the role of personal data in the age of big data. Chapter 3 addresses the relevant aspects of EU rules on data protection, competition and consumer protection. Chapter 4 presents an analysis of the interrelations between the three policy areas:

   - how the control of personal information contributes to market power in the digital economy and the implications for data protection;
   - the risks to the consumer posed by concentrations and the abuse of market dominance where firms process massive amounts of personal data; and
   - how the growth of a vibrant market for privacy–enhancing services[5] can be encouraged by strengthening informed consumer choice.

---

Transatlantic Perspective: Data Protection and Competition Law', in *Data Protection Anno 2014: How to Restore Trust?* eds. Hijmans, H. and Kranenborg, H., 2014, pp. 225-234.

[3] The European Council in October 2013 committed to 'complete the Digital Single Market' by 2015 including 'the right framework conditions for a single market for Big Data and Cloud computing', by developing e-government, e-health, e-invoicing and e-procurement, by the acceleration of e-identification and trust services, e-invoicing and payment services, and by the portability of content and data; http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf. The EDPS has issued an Opinion on the EU umbrella policy programme of Digital Agenda for Europe; https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-04-08_Digital_Agenda_EN.pdf

[4] See EDPS Strategy 2013-2014: 'Towards excellence in data protection'; https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/13-01-22_Strategy_EN.pdf. In addition to Opinions regularly issued in response to legislative proposals or policy documents adopted by the Commission or other institutions or bodies under Article 28.2 of Regulation (EC) No 45/2001, and as part of his role of advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data under Article 41(2), the EDPS may decide to issue advice on his own initiative with a view to contributing to debates on legal and societal developments that may have a major impact on the protection of personal data. For example, see the EDPS Opinion on the relationship between cloud computing and the data protection legal framework, OJ C 253, 3.09.2013, p.1. Similar advice on other areas of concern may be issued.

[5] Privacy-enhancing technologies have been defined by the Commission as 'a coherent system of information and communication technology measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data without losing the functionality of the information system.' 'Promoting Data Protection by Privacy Enhancing Technologies (PETs)', COM(2007) 228 final. In this document, the term 'privacy-enhancing services' is used to refer to customer services which have been designed on the basis of such technology.

The importance of joined-up thinking, enforcement and cooperation between supervisory authorities at international, EU and national level is also emphasised.[6]

5. In conclusion, Chapter 5 looks ahead to possible policy responses, and invites the Commission, national supervisory authorities, advocacy groups and legal practitioners to engage in a broader and deeper discussion on this matter. At the start of each section, bullet points and cross references aim to guide the reader through the key arguments and intersections between the three areas of EU law. A summary of these interfaces is presented in the Annex to this document.

## 2. Big data, personal data: the fuel of the digital economy

- *Companies across all sectors of the economy rely on enormous volumes of personal data for developing services, but unlike other intangible assets, this is rarely accounted for*
- *'Free' online services are 'paid for' using personal data which have been valued in total at over EUR 300 billion and have been forecast to treble by 2020*
- *Despite the risks to the personal data of individuals using these services, the market for privacy-enhancing services remains comparatively weak*

> *Competition in major digital markets often takes on a rather distinctive form. First, competition between business models or platforms tends to be more important than competition within a business model because platform competition often leads to a winner takes all outcome. In other words, dominance - or even monopoly - can be the virtually inevitable outcome of success. Second, digital markets are often characterised by strong network effects and economies of scale, which reinforce this competition-to-dominance trait. Third, many digital markets are two-sided, so that two or more user groups benefit from use of the digital platform. For example, search engines are used both by individuals to access information on the internet and by advertisers to access viewers…*
>
> OECD, The Digital Economy, February 2013.

### *2.1. Big personal data as an asset*

6. The digital economy is marked by strong, dynamic growth, a high turnover of new services, market concentration involving a few overwhelmingly dominant players, and an ever greater imbalance between big companies on the one side, and SMEs and individual users on the other side.[7] This growth has been accompanied, in all sectors of the economy, by an exponential rise in the value of data and advances in data mining and analytics and a massive increase in computing power and data storage capacity.

[6] This includes liaison within and between the Global Privacy Enforcement Network, International Competition Network as well as deeper collaboration between EU authorities and the US Federal Trade Commission.
[7] See EDPS Opinion on the Commission's communication on 'Unleashing the potential of cloud computing in Europe', 16 November 2013.

7. According to a recent survey, 57% of businesses analysed consider themselves to be 'managing big data', in the sense of 'very large datasets' which can include 'streaming data from machines, sensors, web applications and social media'.[8] In a process which has been branded 'datafication', an estimated 2.3 trillion gigabytes of data are collected and combined with other data every day, the data themselves becoming the basis for services such as diverse as fitness trackers and global mapping.[9] Big data is more than personal data: it includes aggregated and anonymous data. Companies may consider most of their data to be non-personal datasets, but in reality it is now rare for data generated by user activity to be completely and irreversibly anonymised.[10] Masses of personal information are generated by over 369m internet users in the EU[11] through their consumption of social media, games, search engines and e-commerce and other services. Information on subscribers to a given online service which is collected includes names, gender, personal preferences, location, email addresses, IP addresses and surfing history. This is used to invest in existing client relations and to acquire new clients.

8. Whereas previously data had been collected as part of the provision of a particular service, 'the added value of big data,' says one commentator, 'resides in the potential to uncover new correlations for new potential uses once the data have been collected … [which] may have nothing to do with the original purposes for which the data were collected.'[12] Estimates of this added value vary according to context and methodology: revenues or net income per record/user for two global companies whose business models rely on personal data have been calculated at EUR 3-5 per year;[13] while the digital value that EU consumers place on their data has been estimated at EUR 315 billion in 2011, forecast to rise to EUR 1 trillion by 2020.[14]

9. The extent to which companies should be able to leverage and to monetise the personal datasets acquired has been the subject of some debate. Nevertheless, personal information has become a substantial intangible asset used for the purposes of value creation, comparable to copyright, patents, intellectual capital and goodwill.[15]

---

[8] The 2013 survey by the Data Warehousing Institute was targeted at 'data management professionals' and drew 693 responses from a range of sectors including financial services, consulting, software/ internet, healthcare and insurance, of whom 48% were based in US and 20% in Europe; Russom, P., 'TDWI Best Practices Report: Managing Big Data', Fourth Quarter 2013.

[9] Source for estimated daily generation of data: IBM. See Mayer-Schönberger, V., and Cukier, K. (2013), Big Data, A Revolution That Will Transform How We Live, Work and Think, pp. 94 – 97.

[10] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 20.06.2007.

[11] Miniwatts Marketing Group (figure based on EU-27).

[12] Moerel L., inaugural address Tilburg Law School, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof', 14.02.2014.

[13] See OECD (2013), Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, No. 220, OECD Publishing. The recently announced acquisition of Whatsapp by Facebook for USD 19 billion is the equivalent of paying EUR 30 for each of the messaging service's 450 million users. The European Commission has still to decide whether this case will be subject to merger control. (http://www.bloomberg.com/news/2014-02-20/facebook-s-whatsapp-deal-seen-avoiding-u-s-antitrust-challenge.html , accessed 10.03.2014.)

[14] Boston Consulting Group, 'The Value of our Digital Identity', November 2012, http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf (accessed 05.03.2014).

[15] This has been recognised by the Commission: 'Today, personal data are a type of asset for companies' (speech by Vice-President Almunia, 'Competition and personal data protection', 26 November 2012); '…big data is not just a new sector, but a new asset class. One that sits as a pillar of our economy, like human resources or financial capital' (speech by Vice-President Kroes, Big Data for Europe, 7.11.2013). See also World Economic Forum publication 'Personal Data: The Emergence of a New Asset Class', 2011. For a definition of an asset, the International Financial Reporting Standards Framework states that 'An asset is a resource

Often it is a company's most valuable asset, as demonstrated by recent high profile initial public offerings on global stock markets and mergers in the digital economy. However, unlike other intangible assets, the value of the personal information under a company's control does not seem to be accounted for on its balance sheet.[16]

### *2.2. A currency for purchasing 'free' services*

10. With many digital services like email or search engines which are used by almost every internet user, companies foster the perception that they are provided for free; in fact individuals are required to surrender valuable personal information to enjoy them. Consumers provide richly detailed information about their preferences through their online activities which permits individuals, not groups, to be targeted with far greater precision than ever before. For consumers, therefore, personal information operates as a currency, and sometimes the sole currency, in the exchange of online services.[17]

### *2.3. Business models designed to capture value of big, personal data*

11. A four-step 'personal data value chain' has been identified,[18] consisting of (1) collection and access, (2) storage and aggregation, (3) analysis and distribution and (4) usage of personal datasets. Across this value chain, a multiplicity of individuals, businesses, public institutions and non-profit organisations might be expected to view and to process these datasets. This includes data brokers, who mediate trade in personal information between one data controller and another,[19] and cloud computing providers (for application and storage services).

12. Often companies rely on and exploit big data by operating on a **two-sided or multi-sided platform or business model**, cross-financing distinct services provided to two or more distinct user groups, that is, users of 'free' services on the one hand, and other businesses and especially advertisers, on the other. Through the supply of payment-free services, these companies compete for the attention and loyalty of individuals whose use of those services will generate personal data with a high commercial value.

---

controlled by the enterprise as a result of past events and from which future economic benefits are expected to flow to the enterprise'. Although it is not the subject of this document, revelations of government surveillance activities has served to further demonstrate that value of personal information goes well beyond commercial concerns.

[16] See OECD, Innovation Strategy and sources of growth.

[17] 'Personal data is the currency of today's digital market;' speech by Vice Commissioner Reding, 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age – Innovation Conference Digital, Life, Design', Munich, 22 January 2012. 'Profit maximising firms do not provide products for free unless it helps them make money somewhere else'; Evans, D., S. (2011), The Antitrust Economics of Free, University of Chicago Working Paper No 555, 2011.

[18] Organisation for Economic Cooperation and Development (OECD), 'Exploring the Economics of Personal Data', 2013.

[19] Data or information brokers collect personal information about consumers and sell that information to other organisations using a variety of public and non-public sources including courthouse records, website cookies and loyalty card programs to create profiles of individuals for marketing purposes, and sell them to businesses who want to target their advertisements and special offers. Apart from the general rights to access applicable under the Data Protection Directive (see paragraph 25) there is no legislation that explicitly requires a data broker to share with their customers either the information they have gathered or the customer profiles developed using those data. In the US this industry is the subject of ongoing enforcement, information-gathering and awareness raising activities by the Federal Trade Commission; see http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-entitled-what-information-do-data-brokers-have-consumers/131218databrokerstestimony.pdf (accessed 10.03.2014).

They may discriminate between users with offerings scaling from free basic services to premium services which target those businesses which are willing to pay for them.[20]

13. More lucratively, these companies may sell the information collected to advertisers, often via data brokers, or purchase space for placing their ads next to search results. Advertising, consulting and statistical services depend on the information gathered by digital companies to create online user profiles which in turn enable more efficient behavioural targeting.[21] This process is quite distinct from marketing approaches in the past, where adverts would for example be targeted at imperfectly segmented groups of TV viewers.

### *2.4. An underdeveloped market for privacy-enhancing services*

14. Big data promises big benefits for society in sectors ranging from entertainment and transport to health and energy conservation; but where it involves personal data it also implies big risks for the individual to whom the information relates.[22] Despite this heightened risk, the market for privacy-enhancing services in the digital economy remains weak. While many consumers may be becoming more and more 'tech savvy', most appear unaware of or unconcerned by the degree of intrusiveness into their searches and emails as information on their online activities is logged, analysed and converted into revenue by service providers. Thus far, relatively few companies in the digital economy have detected financial advantage in enhancing the privacy of their offerings.[23]

## 3. Legal background

- *Separate rules on data protection, competition and consumer protection all converge around a two-fold purpose – the protection and promotion of the welfare of the individual and the facilitation of the creation of a single European market.*

- *The purpose of competition rules is the efficiency of the internal market and the welfare of consumers, and appraisal of those rules must be placed within the general framework of the EU's objectives and values*

- *Consumer protection rules aim to prohibit misleading claims about products and services, particularly those marketed as 'free'*

15. The main objectives of the EU include its core values of promoting peace and the well-being of its peoples, and its economic mission, including an area of freedom without internal frontiers and an internal market where competition is free and undistorted.[24] Rules adopted by the EU on data protection, competition and consumer

[20] These services may be contrasted with internet facilities such as Wikipedia which are genuinely free to use and ad-free although users may be invited to donate money in support.
[21] Geradin, D. and Kuschewsky, M. (2013), 'Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue', SSRN.
[22] See, for example, Pentland, A., *Social Physics* : *How Good Ideas Spread—The Lessons from a New Science*, (Penguin, 2014) and the discussion of benefits and risks in Polonetsky, J. and Omer, T., 'Privacy and Big Data: Making Ends Meet', 66 Stanford Law Review Online, 25, 3.10.2013.
[23] See Section 4.3 below. For a discussion of how 'status quo bias' may induce reluctance to question default 'privacy settings', see Moerel (cited above footnote 12).
[24] Article 3, Treaty on European Union.

protection, applying to economic operators and Member States,[25] reflect those core values and economic mission in distinct ways and under separate legal bases in the Treaty on the Functioning of the European Union (TFEU). There are separate supervisory authorities at national and EU level, and compliance with one set of rules does not necessarily mean compliance with the other, nor does non-compliance with one set imply infringement of the other. The purposes of the three areas however converge, and that point of convergence is the focus of this section.

## *3.1. Data protection*

### 3.1.1. The fundamental right to protection of personal data

*See also: Sections 3.2.1 (aims of EU competition rules) and 3.3.1 (requirement to ensure consumer protection)*

16. The right to respect for private and family life, home and communications as laid down in Article 7 of the Charter of Fundamental Rights protects the individual primarily against interference by the state. Article 8 formulates the protection of personal data as a separate right. It goes beyond simply protecting against interference by the state. It is a proactive right which entitles the individual to expect that his or her information will only to be processed, by *anyone* and not only the state, if certain essential requirements laid down in Article 8 (2) and (3) are fulfilled. This requires that the processing is fair and lawful and for specified purposes, that it is transparent to the individual who is entitled to access and rectification of his/her information, and that the rights must be subject to control by an independent authority.[26]

17. Article 16 TFEU requires rules to be laid down relating to data protection and to the free movement of such data in the internal market. **Directive 95/46/EC** (the 'Data Protection Directive'), although adopted on another legal basis, is currently still the central piece of legislation under this article. It requires a balancing of the control of one's personal information and the free movement of data in the internal market. The European Parliament and the Council are currently discussing the proposals for a new legal framework proposed by the Commission in January 2012.[27] Within this framework, **Directive 2002/28/EC**, contains specific rules on privacy in relation to digital technologies and electronic communications services, noting in particular that 'the successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk' (Recital 5).[28]

[25] Public bodies in Member States in processing personal data are subject to the obligations arising from the Data Protection Directive except in the course of an activity that falls outside the scope of EU law or where the processing concerns public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law; Article 3 of the Data Protection Directive. State aid rules in Articles 107-109 TFEU seek to control actions by Member States themselves, rather than companies, which may distort competition or trade between Member States.

[26] See Kokott, J. and Sobotta, C., 'The Distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', International Data Privacy Law, 2013, Vol. 3, No. 4, pp. 222-228.

[27] Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation) COM(2012)11 final.

[28] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201/37.

18. Personal data as defined in Article 2(a) of Directive 95/46/EC means 'any information relating to an identified or identifiable natural person'. This includes any information which refers to the identity, characteristics or behaviour of an individual or which is used to determine or to influence the way in which that person is treated or evaluated.[29] Identities may be disguised through various techniques, such as key-coded data, but it is usually possible to trace back such 'pseudonymised' information to the individual, and therefore data protection laws will still apply.[30] All individuals as data subjects benefit from this legal protection, whether or not they are deemed to be a consumer of a particular service. In some cases legal persons may also benefit from the protection, for example where the official title of the legal person or other information identifies one or more natural persons.[31]

19. The right to the protection of personal data is not an absolute right but 'must be considered in relation to its function in society'.[32] Under Article 52(1) of the Charter, limitations may be imposed on the exercise of these and other rights so long as the limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

### 3.1.2. Persons subject to obligations under data protection rules

*See also: Section 3.2.2 Scope of application of competition rules.*

20. In the interests of ensuring a level playing field, EU data protection law applies equally to all data controllers established in the EU or using equipment situated in the EU.[33] Under the Commission's proposed general data protection regulation, the territorial scope of the EU's rules would be extended to any data controller 'offering goods or services' and 'monitoring [the] behaviour' of data subjects residing in the EU.[34] This clarification seems appropriate in the light of the global exchanges of information which characterise the digital economy. A comparison may be made to EU competition rules which apply wherever an undertaking's conduct could affect the internal market, irrespective of its place of establishment (see paragraph 32).

---

[29] Working Party document WP 105, Working document on data protection issues related to RFID technology, 19.1.2005, p. 8.

[30] Article 29 Working Party Opinion No 4/2007 on the concept of personal data, WP136, adopted on 20 June 2007pp. 18-21.

[31] See judgment in Joined Cases CJEU, *Volker und Schecke and Eifert v Land Hessen* (C-92/09 and C-93/09), [2010] ECR I-11063, paragraph 53. The Data Protection Directive (Article 2 (a)) provides for protection of the personal data of all identified or identifiable natural persons. This is maintained in the Commission's proposed General Data Protection Regulation (Recital 12 and Article 4 (1)). Certain national jurisdictions (Austria, Denmark, Italy and Luxembourg) extend some protection to legal persons; Korff, D. (on behalf of European Commission), Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons, 1998;
http://ec.europa.eu/justice/policies/privacy/docs/studies/legal_en.pdf.
Directive 2002/58/EC explicitly provides (Article 1(2)) for the protection of the legitimate interests of subscribers to electronic communications services who are legal persons.

[32] *Schecke*, paragraph 48.

[33] Directive 95/46/EC Article 4(1).

[34] See Article 3 (1) and (2). It is worth noting that the EP has sought to clarify that the scope should encompass the offering of goods and services 'irrespective of whether connected to a payment or not' [text added to Recital 20], in an attempt to eliminate any doubt that 'free' online services such as search or social media fall firmly within the scope of the Regulation.

21. All businesses which are data controllers are subject to obligations to protect personal data, irrespective of their size or even dominant position in a market. However, as has been noted recently by the European Court of Human Rights, 'The greater the amount and sensitivity of data held and available for disclosure, the more important [is] the content of the safeguards to be applied at the various crucial stages in the subsequent processing of the data.' Many data protection provisions can therefore be considered scalable in proportion to the volume, complexity and intrusiveness of a company's personal data processing activities, and are therefore of particular relevance to powerful, big data-managing companies.[35] This is analogous to the concept of the 'special responsibility' on the part of dominant undertakings to avoid distortions to competition in the internal market, as will be discussed below (see paragraph 33).[36]

### 3.1.3. Legitimate and compatible purposes for data processing

*See also: Section 3.2.3 Definition of the relevant market*

22. Article 6 (1) (b) of the Data Protection Directive provides that personal data must be 'collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.' This purpose limitation principle is necessary in order to ensure trust, predictability, legal certainty and transparent use of personal data by data controllers.[37] Further processing for a secondary purpose is not forbidden, but the secondary purpose must not be 'incompatible' with the purposes for which the data have been collected. Distinguishing between compatible and incompatible processing of personal data is often a complex and delicate exercise in data protection law. While the directive does not necessarily prohibit processing for different purposes, the Article 29 Working Party recommended that compatibility should be assessed in the light of the context in which the data were collected, of reasonable expectations of the data subjects, of the nature of the personal data in question, of the impact of further processing, and of safeguards to protect the data subject.

23. The concept of compatibility may be compared with that of substitutability, which is used in the application of competition rules to determine which products may be considered to be competing in the same market. In the context of the digital economy, it is conceivable that a company might collect data for the purpose of providing a certain service in one market, and further process those data in order to compete in the provision of another service in a separate market (see paragraph 58).

### 3.1.4. Consent and the rights to information, to access to data and to data portability

*See also: Sections 3.2.4 (Consumer welfare in application of competition rules) and 3.3.2 (Obligation to provide accurate information to customers)*

24. Personal data processing requires a legal basis. One such basis is the freely-given, unambiguous and informed consent of the data subject to the specific processing

[35] ECtHR 13 November 2012, 24029/07, *M.M. v UK*, paragraph 200.

[36] The Commission's proposed General Data Protection Regulation envisages fewer administrative obligations for small and medium enterprises; see Recital 11 of the Commission proposal. According to the draft European Parliament legislative resolution on the proposal, reduced obligations would apply to data controllers processing data related to 5000 or fewer data subjects in a given year.

[37] This section uses the analysis contained in Article 29 Working Party Opinion 03/2013 on purpose limitation, WP 203, adopted on 2 April 2013.

operation.[38] Mere silence or inaction, such as in the case of default settings of online social networks or web browsers, is not valid. Consent should be requested prior to the data processing and only after the data controller has given notice to the data subject of the processing operations in clear and understandable language. It may be withdrawn, in which case any personal data pertaining to the data subject should be erased unless there is another legal basis that justifies continued storage of the data.[39]

25. Individuals are entitled to be told about the processing of their personal information, including the identity of the controller, the purpose(s) of the processing, the recipients of the data, as well as their rights as data subjects.[40] Under Article 12 of the Data Protection Directive, they have the right to access the data relating to them and to obtain rectification, erasure or blocking of the data where it is incomplete or inaccurate. The proposed reform envisages (Article 18) extending this right to enable the data subject to obtain a copy of data being processed electronically, including for example social network profiles, purchase and search histories, and to transmit them to another automated processing system.

26. This right to data portability would allow users to transfer between online services in a similar way that users of telephone services may change providers but keep their telephone numbers.[41] In addition, data portability would allow users to give their data to third parties offering different value-added services. By way of illustration, if applied to smart metering it would enable customers to download data on their energy usage from their existing electricity supplier and then to hire a third party able to advise them whether an alternative supplier could offer a better price, based on their patterns of electricity consumption. Such transparency enables individuals to exercise their other data protection rights and may be seen to mirror the objective of rules on the provision of clear and accurate information to the consumer (see section 3.3.2).

### 3.1.5. Supervision, enforcement, sanctions and access to remedies for infringements

*See sections 3.2.5 and 3.3.3 on supervision etc.*

27. Article 8(3) of the Charter asserts that the rules laid down 'shall be subject to control by an independent authority'. Article 16 (2) TFEU provides for the laying down of rules on data protection whose compliance is to be 'subject to the control of independent authorities'. Article 28(1) of Data Protection Directive duly requires EU Member States to provide for one or more public authorities to act with complete independence in the monitoring of the application of the directive.[42] Data protection authorities' tasks include dealing with complaints and conducting investigations. They

[38] Article 2 (h) Data Protection Directive. See Article 29 Working Party Opinion 15/2011 on the definition of consent, WP187, Adopted on 13 July 2011.
[39] This is implicit within the Data Protection Directive and explicit in the e-Privacy Directive Articles 6(3) and 9 (1) regarding the processing of traffic and location data by publicly available electronic communications services.
[40] Directive 95/46/EC Article 10
[41] 'Number portability' is provided for by Article 30 of Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).
[42] Directive 95/46/EC Article 28. The European Court of Justice has given a wide interpretation to the requirement for complete independence of data protection authorities in *Commission v. Germany*, C-518/07) and *Commission v. Austria*, C-614/10. See also Article 47 of the proposed General Data Protection Regulation, COM (2012) 11 final.

may order the blocking, erasure or destruction of data and temporary or definitive bans on processing.

28. Every person has the right to a judicial remedy for any violation of the rights guaranteed under the directive (Article 22) and to receive compensation for any damage suffered as a result of unlawful data processing (Article 23). The sizes of potential sanctions for breaches vary widely between Member States: the lower limit in Croatia is HRK 10 000 (EUR 1 131), while the UK authority may require penalties of up to GBP 500 000 (EUR 597 000). In practice victims of unlawful processing are prevented from obtaining redress through the length and expense of proceedings and lack of unawareness of data protection rules and rights, although there have been some encouraging developments.[43] The Regulation proposed by the Commission also envisages administrative sanctions as a proportion of a company's annual turnover which would be applicable in the case of breaches of data protection obligations, such as unlawful disclosure to another organisation.[44] This appears to follow the approach to sanctions applicable in the case of anti-competitive agreements (see paragraph 45 below).

29. Unlike for merger cases under competition rules (see paragraph 52 below), where a data protection problem arises affecting individuals in more than one Member State, the company in question may currently be subject to investigation by several national authorities with often diverging outcomes. National authorities convene as an independent advisory body known as the Article 29 Data Protection Working Party, whose tasks include promoting a uniform application of the general principles of the Data Protection Directive, but which has no formal role in enforcement. Measures for ensuring consistency have therefore been envisaged in the proposed General Data Protection Regulation[45] whereby only one authority would be responsible for taking legally binding decisions against a company, authorities would be obliged to cooperate and a new European Data Protection Board would consider matters with an EU-wide impact.

## *3.2. Competition*

### 3.2.1. Aims of EU rules on competition

*See Sections 3.1.1 (Fundamental right to data protection) and 3.3.1 (Requirement to ensure consumer protection)*

30. Competition law concerns the behaviour of companies and abuse of market power. It has long been of central importance to the EU and has evolved through several phases: it initially functioned as a means of preventing public obstacles to interstate trade, and now it seeks to ensure necessary controls of corporate mergers and liberalisation of sectors of the public economy.[46] Its principal aims are to enhance the efficiency of the internal market and the welfare of and choice available to

[43] Fundamental Rights Agency, Access to data protection remedies in EU Member States, 2013. In February 2014 the German federal government announced its intention to allow consumer rights organisations to sue business directly for breaches of national data protection rules; http://www.spiegel.de/netzwelt/netzpolitik/verbraucherschutzminister-maas-kuendigt-verbandsklagerecht-an-a-952767.html

[44] Articles 31 and 32, COM(2012)11 final .

[45] Article 58-63 COM(2012)11 final.

[46] Wesseling, R. (2000), *The Modernisation of EC Antitrust Law*, pp. 48-9.

consumers.[47] It has even been argued that the ultimate purpose of competition law is to ensure that the internal market will satisfy all reasonable wishes of consumers for competition, including not only the wish for competitive prices but also the wish for variety, innovation, quality and other non-price benefits, including privacy protection.[48]

31. To these ends, Articles 101-106 TFEU prohibit agreements between companies which would prevent or distort competition, seek to prevent abuse of a dominant position, and require the Commission to investigate cases of suspected infringement of the principles of competition. Articles 107-109 TFEU also aim to ensure a level playing field across the internal market by preventing preferential treatment by Member States to certain companies. The EU is able to adopt appropriate regulations or directives in the application of these principles and rules (Articles 103, 106 and 109), of which the most significant are **Council Regulation (EC) No 1/2003 (the 'Modernisation Regulation')**, which decentralised application of competition rules to national authorities, and **Council Regulation (EC) No 139/2004 (the 'Merger Regulation)** along with Implementing Regulation (EU) No 1269/2013 which contain the main rules and procedures for the assessment of concentrations.[49]

### 3.2.2. Scope of competition rules and market power

*See also: 3.1.2 Persons subject to data protection obligations*

32. EU competition rules apply wherever any 'economic activity' may 'affect trade between Member States'; its scope is not bounded by the place of establishment of a given company.[50] Enforcement of these rules often involves an assessment of the market power of a given undertaking and of whether the undertaking occupies a dominant position. The Commission evaluates market power and market structure through an assessment of market share, that is, the relative importance of the various undertakings active on the market.[51] The usual determinant in the assessment of market share is company turnover, or volume or value of total sales of the relevant product in the relevant area. Market share is then interpreted in the light of the

[47] The CJEU defined the concerns of competition law to be consumer welfare, the interests of competitors and the structure of the market; Joined Cases CJEU, *GlaxoSmithKline Services Unlimited, formerly Glaxo Wellcome plc vs Commission* C-501/06P, C-515/06P and C-519/06P), [2009] ECR I-9291, paragraph 6.

[48] 'First, privacy harms reduce consumer welfare, which is a principal goal of modern antitrust analysis. Second, privacy harms lead to a reduction in the quality of a good or service, which is a standard category of harm that results from market power;' Swire, P., 'Protecting Consumers: Privacy matters in antitrust analysis', CCTr. for Am. Progress, 19.10.2007. See also Lande, R., 'The Microsoft-Yahoo Merger: Yes, Privacy is an Antitrust Concern', FTC: Watch, No. 714, 2008, University of Baltimore School of Law Legal Studies Research Paper No. 2008-06; and Averitt, N., Lande, R. and Nihoul, P., '"Consumer choice"' is where we are all going – so let's go together', Foreword, Concurrences No 2-2011.

[49] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1, 04.01.2003, p.1-25; Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation), OJ L 24, 29.1.2004 (hereafter referred to as 'the Merger Regulation'); Commission Implementing Regulation (EU) No 1269/2013 of 5 December 2013 amending Commission Regulation (EC) No 802/2004 implementing Council Regulation (EC) No 139/2004 on the control of concentrations between undertakings, OJ L 336, 14.12.2013, pp. 1-36.

[50] Commission Notice Guidelines on the effect on trade concept contained in Articles 81 and 82 of the Treaty, 2004/C 101/07.

[51] Communication from the Commission, Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, 2009/C 45/02.

specific conditions of the market:[52] for measuring market share in one specific sector relevant to the digital economy, Commission guidelines recommend the selection of whichever criteria are most appropriate in the light of the characteristics of the market.[53]

33. Market dominance becomes likely, though not inevitable, where an undertaking's market share equals or exceeds 40%.[54] The Commission also considers barriers to expansion or entry into the relevant market, listing as examples economies of scale, privileged access to essential inputs, and costs or other impediments to customers switching to new suppliers.[55] Case law has established that a dominant undertaking has a 'special responsibility' not to conduct itself in such a way that harms competition:[56] it may seek to protect its own interests under attack from competitors but not to strengthen its dominant position.

### 3.2.3. Definition of the relevant market

*See 3.1.3 Legitimate and compatible purposes for data processing*

34. The definition of the relevant market is the first stage in the legal analysis of cases of anti-competitive agreements, mergers and abuse of dominant market position. This allows competition regulators to identify the market operators, that is, suppliers, customers and consumers, and to calculate the total market size and the market share of each supplier with reference to the relevant product or service in the relevant area. This exercise in general considers three variables:

    a. the product market, including products and services which are considered by consumers to be interchangeable or substitutable; this consideration includes supply side substitutability, that is, the possibility of switching on the production side;

    b. the geographic market, the area where generally similar competition conditions prevail which are distinct from neighbouring areas; and

    c. a time horizon, reflecting the changes in consumer habits and technological developments.[57]

[52] Paragraph 13 of Commission guidance 2009/C/ 45/02.

[53] 'The criteria to be used to measure the market share of the undertaking(s) concerned will depend on the characteristics of the relevant market. It is for NRAs to decide which are the criteria most appropriate for measuring market presence. For instance, leased lines revenues, leased capacity or numbers of leased line termination points are possible criteria for measuring an undertaking's relative strength on leased lines markets'; Commission guidelines on market analysis and the assessment of significant market power under the Community regulatory framework for electronic communications networks and services, 2002/C 165/03, OJ C 165, 11/07/2002. The issuing of this guidance was a requirement of Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services.

[54] Paragraph 14 of Commission guidance 2009/C 45/02. The CJEU has considered other factors in considering the dominance or otherwise of undertakings; see CJEU cases C-27/76 *United Brands Company and Unit Brands Continental BV v. Commission* [1978] and C-85/76 *Hoffmann-La Roche and Co. AG v. Commission* [1979].

[55] Paragraph 16-18 of Commission guidance 2009/C 45/02.

[56] Paragraph 9 of Commission guidance 2009/C 45/02.

[57] Commission Notice on the definition of relevant markets for the purposes of Community competition law, 97/C 372/03, OJ C372/5. Commission Decision of 24 July 1991 relating to a proceeding pursuant to Article 86 of the EEC Treaty (IV/31043 - Tetra Pak II) 92/163/EEC, OJ L 072, 18.03.1992.

35. The Commission, in determining substitutability, has some flexibility in this area. It considers not only product characteristics and intended use but also other factors, including the views of customers and competitors, evidence of customer preferences and the existence of different categories of customers for the product.[58]

### 3.2.4. The notion of consumer welfare in the application of competition rules

*See sections 3.1.4 (Consent and rights to information etc.) and 3.3.2 Obligations of fairness and accurate information)*

36. Consumer welfare has not been defined in EU law and its relationship with market efficiency is not commonly understood.[59] The European Court of Justice has rarely referred to consumer welfare in its judgments on competition cases.[60] That said, as the Commission recognises in its guidelines on enforcement of rules on abuse of dominance,[61] welfare is determined not only by price, but also by other factors, such as quality and consumer choice, which is also a relevant concern for data protection. In addition, concern for the interests of the consumer recurs, at least at a conceptual level, in each major branch of competition law, namely:

    a. the prohibition of anticompetitive agreements;

    b. combating abuse of a dominant market position, through exclusionary conduct (such as refusal to supply a product or service which is necessary to compete) or exploitation;

    c. control of mergers; and

    d. control of state aid.

*a) Anticompetitive agreements*

37. Article 101 TFEU prohibits agreements between undertakings, which affect trade between Member States and whose object or effect is the prevention, restriction or distortion of competition. Certain agreements are permitted where they contribute 'to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit' in line with the conditions of Article 101(3) TFEU.

[58] Paragraphs 36-43 of Commission notice 97/C 372/03.

[59] Economists generally understand consumer welfare as the individual's own assessment of his/her satisfaction with benefits derived from the consumption of goods and services as compared with prices and income. Exact measurement of consumer welfare therefore requires information about individual preferences; see for example OECD Glossary of Industrial Organisation Economics and Competition Law. See Skourtis, A. (2012), Is consumer welfare the (only) way forward? A re-appreciation of competition law objectives ante portas in both US and EU, University of Reading, Centre for Commercial Law and Financial Regulation, August 2012. Arguments have been advanced that competition policy should take account of wider social and political aims; e.g. Stucke, M, E., 'Reconsidering Antitrust's Goals', Boston College Law Review, Vol. 53 2012, pp. 551-629; Stucke, M. E., 'Reconsidering Competition', Mississippi Law Journal, Vol. 81, 2011, pp. 107-188.

[60] Akman, P. (2008), '"Consumer welfare" and Article 82EC: Practice and rhetoric', CCP Working Paper 08-25, July 2008.

[61] Article 19 of Commission Guidance 2009/C 45/02.

*b) Abuse of market dominance: exclusionary conduct, refusal to supply, essential facilities and exploitation*

38. Dominance in competition terms involves the ability to determine prices and to control production in a given market. Dominance in a relevant market does not in itself constitute an infringement of competition rules.[62] However, the abuse of a dominant market position which affects trade between Member States is prohibited under Article 102 TFEU. Such abuse has tended to be understood[63] as taking one of two forms: [64]

    i. *exclusionary conduct*, where a dominant undertaking excludes actual or potential competitors by means other than competing on the merits of the products or services they provide; and

    ii. *exploitation*, or action which 'directly' harms consumers through, for example, charging excessively high price.

    The Commission has issued enforcement guidance in relation to exclusionary conduct[65] by dominant undertakings.

39. **Exclusionary conduct** is abusive where it results in 'foreclosing [the dominant undertaking's] competitors in an anti-competitive way' and therefore potentially damages the competitive market structure.[66] The Commission's guidance identifies specific forms of exclusionary conduct, namely, exclusive dealing, **tying** and **bundling**, predation and refusal to supply and market squeeze.[67] Examples may involve selling at such a low price to customers that other firms are deterred from entering the market (bundling), or obliging the customers of one popular service to purchase another of the seller's services which the customer has not requested (tying). Such actions are deemed to be 'most harmful to consumers' and to have 'adverse

[62] 'Therefore, whilst the finding that a dominant position exists does not in itself imply any reproach to the undertaking concerned, it has a special responsibility, irrespective of the causes of that position, not to allow its conduct to impair genuine undistorted competition on the common market (Case T-203/01 *Michelin v Commission* [2003] paragraph 57). Similarly, whilst the fact that an undertaking is in a dominant position cannot deprive it of its entitlement to protect its own commercial interests when they are attacked, and whilst such an undertaking must be allowed the right to take such reasonable steps as it deems appropriate to protect those interests, such behaviour cannot be allowed if its purpose is to strengthen that dominant position and thereby abuse it; Case 27/76 *United Brands v Commission* [1978] ECR 207, paragraph 189; Case T-65/89 *BPB Industries and British Gypsum v Commission* [1993] ECR II-389, paragraph 69; Joined Cases T-24/93 to T-26/93 and T-28/93 *Compagnie maritime belge transports and Others v Commission* [1996] ECR II-1201, paragraph 107; and *Irish Sugar v Commission*, paragraph 112.

[63] Whish, R. (2012), *Competition Law*, 7th ed., 2012, pp. 201.

[64] Paragraphs 6-7 of Commission guidance 2009/C 45/02.

[65] 'The aim of the Commission's enforcement activity in relation to exclusionary conduct is to ensure that dominant undertakings do not impair effective competition by foreclosing their competitors in an anti-competitive way, thus having an adverse impact on consumer welfare, whether in the form of higher price levels than would have otherwise prevailed or in some other form such as limiting quality or reducing consumer choice. In this document the term 'anti-competitive foreclosure' is used to describe a situation where effective access of actual or potential competitors to supplies or markets is hampered or eliminated as a result of the conduct of the dominant undertaking whereby the dominant undertaking is likely to be in a position to profitably increase prices to the detriment of consumers. The identification of likely consumer harm can rely on qualitative and, where possible and appropriate, quantitative evidence. The Commission will address such anti-competitive foreclosure either at the intermediate level or at the level of final consumers, or at both levels;' paragraph 19 of guidance 2009/C 45/02.

[66] Paragraphs 5 and 19 of Commission guidance 2009/C 45/02.

[67] Paragraphs 75-90 of Commission guidance 2009/C 45/02.

impact on consumer welfare', although there is no explanation of how or why this might occur.

40. One form of exclusionary conduct, **refusal to supply**, contains the concept of an '**essential facility**'.[68] An essential facility is 'a product or service that is objectively necessary to be able to compete effectively' and for which there is no alternative product or service and where technical, legal or economic obstacles make it impossible or unreasonably difficult to develop an alternative.[69] 'Refusal to supply such a facility is likely to lead to elimination of effective competition' or to consumer harm. Consumer harm is likely to arise, 'for instance… where the competitors that the dominant undertaking forecloses are, as a result of the refusal, prevented from bringing innovative goods or services to the market, and/or where follow-on innovation is likely to be stifled,' particularly where the competitor 'intends to produce new or improved goods or services for which there is a potential consumer demand or is likely to contribute to technical development.'[70]

41. Abusive **exploitation** which most obviously could harm the consumer, such as the application of excessive prices or unfair discrimination, has not been addressed by means of Commission guidance. It has rarely been confronted by competition authorities and in most cases of exploitation the 'victims' have been companies, not end consumers.[71] Case law however has established that excessive pricing would be charging a price which has no reasonable relation to the economic value of the product supplied.[72] The CJEU also set out a two-stage test in accordance with which the Commission is required to determine whether:

    (a) the amount of the profit margin is excessive by comparing the disputed price with production costs and, if so, whether

    (b) the price is either (i) unfair in itself or (ii) unfair when compared to competing products.

*c) Merger control*

42. Council Regulation (EC) No 139/2004 ('the Merger Regulation')[73] applies to **mergers** with a 'Community dimension', which bring about 'significant structural

[68] The essential facilities doctrine originated in US case law and states that owners of essential facilities are obliged to deal (the 'obligation to supply') with competitors. It has not been explicitly cited by CJEU, but in C-7/97 *Bronner v Mediaprint Zeitungs* [1998], the court restricted the obligation to supply to situations in which the owner of an indispensable facility held more than a dominant position. The CJEU introduced also a forward-looking test on whether the refusal to supply would lead to monopolisation of a downstream market; see Evrard, S. J. (2004), 'Essential facilities in the European Union: Bronner and beyond', Columbia Journal of European Law 491, 2004.

[69] See *Bronner* and Case C-418/01 *IMS Health v NDS Health* [2004], where the 'essential facility' may be understood as the units of information or 'bricks' concerning pharmacies and doctors used by a dominant undertaking to analyse sales of drugs according by geographical area, for which it owned a copyright under one Member State's law. Theoretically, any competing company could build its own 'brick structure', but the dominant undertaking was judged to have acquired this brick structure in question by means of network effects and a high degree of economic participation by the users of the brick structure (paragraph 30).

[70] Paragraph 87 of Commission guidance 2009/C 45/02. The significant CJEU ruling in this area remains case Case T-201/04 [2007] *Microsoft v Commission*.

[71] Hubert, P, and Combet, L., 'Exploitative abuse: The end of the Paradox?', Doctrines l Concurrences N° 1-2011, pp. 44-51.

[72] Case 27/76, *United Brands v Commission* [1978] ECR 207, paragraph 250.

[73] See footnote 49.

changes, the impact of which on the market goes beyond the national borders of any one Member State'. A merger with a Community dimension falls within the scope of the Regulation and is accordingly appraised by the Commission if the aggregate turnover of the combined undertakings exceeds specified thresholds.[74] The EU merger control regime has the aim of controlling corporate concentrations (more commonly referred to as 'mergers' or 'mergers and acquisitions') and their effect on competition, also taking into account other factors including the 'interests of intermediate and ultimate customers'.[75] In the Google/DoubleClick case, the Commission affirmed that it had referred 'exclusively' to the likelihood that the merger would impede effective competition in the common market, although it also noted that its decision was without prejudice to the merged entity's obligations under the Data Protection Directive.[76]

*d) Exemptions to state aid*

43. Under Article 107 TFEU, **state aid** is defined as any transfer of Member State resources which creates a selective advantage for one or more business undertakings, has the potential to distort trade between in the relevant business market and affects trade between the Member States. Such practice is unlawful, but a number of exemptions apply, for example in the case of environmental protection where undertakings may lack incentives to reduce their pollution due to the cost of doing so.[77] A conceivable case could be advanced for state aid to support the nascent industry for privacy-enhancing technologies and services in the EU.[78]

### 3.2.5. Supervision, enforcement, sanctions and access to remedies for infringements

*See sections 3.1.5 and 3.3.3 on supervision etc.*

44. Competition rules are enforced either by national competition authorities or by the Commission. For mergers, this depends on whether there is a Community dimension. For anticompetitive agreements or abuse cases, the authority which is 'well–placed' will deal with the case in question.[79] Competition authorities may take broader policy considerations into account.[80] In this connection, the Commission is required under the Treaties (Article 2 TEU and Article 2 TFEU) to 'place its appraisal within the general framework' of the EU's objectives and values, which includes of course the rights to privacy and to data protection. Competition authorities have appeared to favour a narrow interpretation focusing on objective economic efficiencies in a

[74] Article 1, the Merger Regulation. The Commission is required to report on the operation of these thresholds and may propose their revision.
[75] Article 2 (1) (b), the Merger Regulation.
[76] Case COMP/M.4731 Google/DoubleClick. DoubleClick was a provider of ad-serving technology, namely, software used to ensure that correctly targeted ads appear on the web page a certain user is viewing.
[77] Recital 45, Commission Regulation (EC) No 800/2008 of 6 August 2008 declaring certain categories of aid compatible with the common market in application of Articles 87 and 88 of the Treaty (General block exemption Regulation).
[78] The Commission intends in 2014 to complete its programme of state aid modernisation in key sectors; Annexes to Commission Work Programme 2014, COM(2013) 739 final, 22.10.2013, p.6.
[79] Cases are allocated through the European Competition Network (see footnote 84).
[80] See http://www.utrechtlawreview.org/index.php/ulr/article/view/URN%3ANBN%3ANL%3AUI%3A10-1-101035/16; http://cadmus.eui.eu/bitstream/handle/1814/22688/2012_guidi_authorversion.pdf?sequence=1

competitive internal market, though consumer welfare considerations may be 'in the ascendancy'.[81]

45. The rules are backed up by a robust sanctions regime. For example, an undertaking found to have infringed rules on anti-competitive agreements may be liable to a fine of up to 10% of its total group turnover in the preceding business year.[82] However, there is currently no harmonisation of rights for consumers either collectively or individually to seek before a court an end to an infringement of competition rules or compensation following such an infringement, though such claims may be brought before national courts.[83]

46. The European Competition Network acts as a forum for discussion and cooperation between regulatory authorities in cases where Articles 101 and 102 TFEU are applied.[84] It aims to ensure an efficient division of work and an effective and consistent application of EC competition rules. The network includes groups of experts in specific sectors including IT, information and communication.

### *3.3. Consumer protection*

#### 3.3.1. The requirement to ensure a high level of consumer protection

*See sections 3.1.1 (fundamental right to data protection) and 3.2.1 (aims of EU competition rules)*

47. EU consumer protection law aims to remove barriers to the internal market by building trust in products and services throughout the internal market, on the basis of transparency and good faith.[85] Article 38 of the Charter requires EU policies to ensure a high level of consumer protection. Article 12 TFEU requires consumer protection to be taken into account in defining and implementing EU policies and activities generally. Article 169 TFEU states that the EU should contribute to the protection of the health, safety and economic interests of consumers and to the promotion of their right to information, to education and to organise themselves to safeguard their interests.

48. The EU has duly adopted various measures for the protection of users of products and services wherever in the internal market they are supplied or consumed. Each measure has been justified on the grounds that diversity of standards and consumer confidence has a deleterious effect on the smooth functioning of the internal market and distorts

[81] Whish (2012), p.19. In the United States which has tended to take a sectoral approach to privacy legislation and where there is no single data protection measure comparable to the EU's Data Protection Directive, competition regulation has also tended towards a purist approach: 'Not only does the Commission lack legal authority to require conditions to this merger that do not relate to antitrust, regulating the privacy requirements of just one company could itself pose a serious detriment to competition in this vast and rapidly evolving industry;' Statement of Federal Trade Commission concerning Google/DoubleClick, FTC File No. 071-0170.

[82] Article 23(2) of Council Regulation No 1/2003.

[83] CJEU, Joint Cases C-295/04 – 298/04, *Manfredi ea v Lloyd Adriatico ea*, [2006] ECR I-6619. The Commission is enquiring into private enforcement and has proposed a draft directive in this field; Proposal for a Directive of the European Parliament and of the Council on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union, COM(2013) 404 final.

[84] Established by Commission Notice on cooperation within the Network of Competition Authorities, 2004/C 101/03, OJ C 101, 27.04.2004.

[85] See section 3.3.2. The term 'consumer' according to EU secondary legislation means 'any natural person who is acting for purposes which are outside his trade, business, craft or profession'.

competition, whereas common standards, choice and fairness are beneficial. The most recent multi-annual programme of action highlights the need for accurate information and market transparency, the promotion of consumers' welfare in relation to price, choice, quality, diversity, affordability and safety and the protection of consumers from potential risks.[86]

### 3.3.2. Obligations of fairness and provision of accurate information

*See sections 3.1.4 (consent and right to information etc.) and 3.2.4 (consumer welfare in competition rules)*

49. In consumer contracts, suppliers have the advantage in defining terms which are not negotiated with individual customers. The **Directive on Unfair Contract Terms**[87] therefore introduced the notion of 'good faith' and required contract terms to be drafted in plain and intelligible language, with any doubt about the meaning of a term to be interpreted in favour of the consumer. Under the **Price Indication Directive**[88] traders are required to provide the selling price in a way that is easily identifiable and clearly legible. The **Consumer Rights Directive**[89] goes further in its aim to eliminate hidden charges and costs in 'off-premises' transactions, particularly those over the internet, such as where individuals are deceived into paying for services presented as 'free'. It requires traders to inform customers in a 'clear and comprehensible manner' of the 'total price of the goods or services… or where the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated….' (Article 6 (e)). More specifically traders are required to provide information on the content of digital services[90] such as their compatibility with hardware and software.

50. The **Unfair Commercial Practices Directive**[91] defines misleading commercial practice as that which omits information (including price) that the average consumer needs to take an informed transactional decision and which thereby causes, or is likely to cause, the average consumer to take a transactional decision that he would not have taken otherwise. Such a misleading omission would include instances where a trader 'hides or provides in an unclear, unintelligible, ambiguous or untimely manner such material information … or fails to identify the commercial intent of the commercial practice if not already apparent from the context' (Article 7). It is misleading for example to describe a product as 'free' or 'without charge' when the consumer has to

[86] Decision No 1926/2006/EC of the European Parliament and of the Council of 18 December 2006 establishing a programme of Community action in the field of consumer policy (2007-2013).
[87] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.
[88] Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers.
[89] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance.
[90] Digital content is defined as 'data which are produced and supplied in digital form, such as computer programs, applications, games, music, videos or texts, irrespective of whether they are accessed through downloading or streaming, from a tangible medium or through any other means'; Recital 19, Directive 2011/83/EU.
[91] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, OJ L 304, 22.11.2011.

pay anything other than the unavoidable cost of responding to the commercial practice and collecting or paying for delivery of the item, or falsely to create the impression that the trader is not acting for purposes relating to his trade, business, craft or profession (Annex I). This is complemented by the **Misleading and Comparative Advertising Directive**,[92] which requires Member States to take steps to combat misleading advertising and permits comparative advertising on condition that it is objective and does not create confusion between traders and competitors.

51. Finally, the EU has put in place general and sector-specific safeguards against risks to consumer health and safety. The **General Product Safety Directive**[93] defines as 'safe' any product which 'under normal or reasonably foreseeable conditions of use… does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons, taking into account … in particular: (i) the characteristics of the product… (iii) the presentation of the product… (iv) the categories of consumers at risk when using the product, in particular children and the elderly'.

52. The provision of clear information about the cost and value of a service to the customer is thus consistently emphasised in the various instruments. This mirrors the right of the individual under the Data Protection Directive to obtain information on data processing 'in an intelligible form'. The concern for product safety, meanwhile, complements both the concept of the exploitation in competition law and the stress in the proposed General Data Protection Regulation on impact assessment,[94] and subsequent discussions on a progressive risk-based approach and on the principle of accountability.[95]

### 3.3.3. Supervision, enforcement, sanctions and access to remedies for infringements

*See sections 3.1.5 and 3.2.5 on supervision etc.*

53. National authorities are responsible for enforcement of consumer protection rules in the EU. Few authorities have the power to obtain monetary compensation for customers.[96]

54. There is no common EU approach to investigation of breaches of consumer law, except in the case of 'intra-Community infringements', that is, any act or omission that 'harms, or is likely to harm, the collective interests of consumers residing in a Member State or Member States other than the Member State where the act or omission originated or took place'.[97] For that purpose Member States are required to designate competent authorities with a duty to cooperate with each other to ensure compliance with those rules, the smooth functioning of the internal market and the protection of consumers' economic interests. These authorities have the right to

[92] Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising.
[93] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ L 011, 15.01.2002.
[94] Article 33, COM(2012) 11 final.
[95] See 'Additional EDPS comments on the data protection reform package', 15.03.2014.
[96] See OECD, 'Consumer Dispute Resolution and Redress in the Global Marketplace', 2006.
[97] Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation).

investigate suspected intra-Community infringements, to request that the seller or supplier concerned cease the infringement and to require a 'payment' from 'the losing defendant' in the event of failure to comply with a court decision.

55. National authorities in the European Economic Area form the Competition Protection Cooperation (or 'CPC') Network[98] which each year identifies common enforcement priorities and carries out concerted enforcement activities including simultaneous checks on compliance with consumer rules, including joint projects on specific sectors. This framework for cooperation is currently under review.

### *4. Interfaces between competition law, consumer protection and data protection*

- *The market for free services in an increasing number of sectors of the digital economy has yet to be analysed but clearly power is achieved through control over massive volumes of data on service users*

- *The scope for abuse of market dominance and harm to the consumer through refusal of access to personal information and opaque or misleading privacy policies may justify a new concept of consumer harm for competition enforcement in digital economy.*

- *Application of competition rules to digital markets has potential to promote privacy-enhancing services and greater consumer control over their own data*

56. The previous section has outlined the main features of data protection, competition and consumer protection rules where common concerns emerge. The present section brings a sharper focus to *four aspects of this policy convergence* against the background of these markets for services relying on personal information. It is argued that in these areas privacy and the protection of personal data should be considered not as peripheral concerns but rather as central factors in the appraisal of companies' activities and their impact on competiveness, market efficiency and consumer welfare.

### *4.1. Relevant markets and market power in the digital economy*

*See sections 3.1.3 (legitimate and compatible purposes for data processing) and 3.2.3 (definition of the relevant market)*

[98] Commission communication pursuant to Article 5(2) of Regulation (EC) No 2006/2004 of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws, concerning the competent authorities and single liaison offices, OJ C 185, 23.06.2012.

*Online 'freemium' games are available cost free if users register by disclosing personal details. These games monitor online activity to learn how to convert free riders into paying customers, or to deliver targeted, more lucrative forms of advertising. A small minority of users pay for additional features but still a sizeable portion of revenue is generated by 'freeriders' or 'non-paying' players. In the EU 46% of users of social networking or sharing sites felt insufficiently informed about the possible consequences of disclosing personal information. The UK's Office for Fair Trading has also been investigating in-game app payments and has identified possible consumer law breaches, not least in the use of what may amount to the use of emotional blackmail, with a view to establishing a common approach to raising industry standards across the world.*

Sources: EU Kids Online, 'Zero to Eight: Young Children and their Internet Use', August 2013; Hoofnagle and Whittington, 'Free: Accounting for the Costs of the Internet's Most Popular Price'; Eurobarometer 359; OFT website.

### 4.1.1. Markets for services paid for by personal information

57. A full market analysis for any of the 'free' digital services has yet to be carried out.[99] In the Commission's analysis of the Google/ DoubleClick merger, only paid-for services, that is, direct sale of online advertising space, intermediary services in online advertising and provision of display ad serving technology, were identified as relevant.[100] Since that case was closed, the evolution of the digital economy has been marked by an explosion of data collection. An equivalent, relevant market analysis today would examine new business models and assess the value of personal information as an intangible asset. It could be expected to reveal the need for undertakings to collect huge amounts of data to be able to monetise the service provided, mainly through advertising, and at the same time to compete with other paid-for service providers.

58. A competition analysis might also consider the substitutability of products and services, taking into account the views of customers and competitors and evidence of customer preferences, in line with existing Commission guidelines. Powerful suppliers of various digital services may initially collect personal data on a massive scale in one market to provide a certain service in that market. One of these suppliers could then process these data, which in competition terms could be defined as input, to supply another service and/or sell the data for processing by another firm which provides services in another distinct market. If, according to the analysis, the 'second' type of service using the data as an input belongs to a separate market, then this service would be deemed non-substitutable with the service for which the data were originally collected. Thus, competition analysis could support the conclusion, from a data protection perspective, that data are being processed for separate and possibly incompatible purposes unbeknown to the individuals who have supplied the data. Such a conclusion could be more evident in cases where the two types of services are perceived by customers to be very different. The application of competition rules could therefore help highlight instances of breaches of data protection law.

[99] See speech by Vice-President Almunia (footnote 2).
[100] See above footnote 76.

59. The analysis would need to take account of the speed of evolution in technology markets. Company expansion and broadening of their range of services can blur the borders between markets. Technological convergence has turned hitherto complementary products into substitutes: hand-held devices for example now compete directly with laptop and desktop computers, which was not the case 10 years ago. Furthermore, geographic markets in the digital economy can be elusive as certain services, such as search, email and file sharing, are not confined to a particular area or state but rather homogeneously available throughout the global online environment.[101]

### 4.1.2. Measuring digital market power

60. Having defined relevant markets for these services, the next stage would be the assessment of market power. Power in the digital economy is partly driven by the degree to which a given undertaking can actually, potentially or hypothetically collect and diffuse personal information. Measuring control of personal information would be a challenging exercise. A relevant market share held by a provider of a free online service cannot easily be calculated by reference to data on traditional sales or volume. These difficulties could be surmounted if competition, consumer protection and data protection authorities were to collaborate in identifying scenarios and in developing a standard for measurement of market power in this area. This standard could then be used to assess suspected infringements in the three areas.

61. Whether or not breaches of both competition and data protection rules were to be established, a deeper appreciation of these markets and of the purposes for which personal information is processed would benefit enforcement. Better informed regulators would be better able to detect practices by dominant market players which are anti-competitive, unfair or which fail to provide accurate information to the consumer. The implications for consumer welfare should therefore become clearer. If regulators fail to acknowledge the increasing importance of personal information as an intangible asset, more and more services reliant on mass personal data processing could in effect be 'ring-fenced' outside the scope of enforcement of consumer protection and competition rules.

[101] The online advertising market, on the other hand, has been assessed to be divided according to national and linguistic borders; Brockhoff, J. et al, 'Google/Double Click: The first test for the Commission's non-horizontal merger guidelines', Competition Policy Newsletter No. 2, 2008.

### *4.2. Digital market power and consumer welfare considerations*

*A dominant firm in the market for email services launches a new photo-sharing platform. The product is offered for free in a bundle with the email service. Users of the email service are nudged into downloading and using the platform without serious consideration. The firm's opportunities for monitoring and profiling user behaviour are thereby enhanced. Customers become more dependent on the photo-sharing service with each uploaded image and each link to any of these pictures they put on their social media profiles, and a while later the firm begins to require payment for an upgrade to a 'premium' version of the service and weakens data protection controls through the imposition of a revised privacy policy for the 'free' version. Customers are effectively locked into the service due to the time and effort it costs them to recover or to recreate the data required to move to an alternative provider. Meanwhile, incentives for potential competitors to enter the market are diminished because they are unable to attract a critical mass of users in order to compete. This might raise questions of exclusionary conduct through tying, or even exploitation, were the 'price' paid through the surrender of personal information to be considered excessive in relation to the value of the service consumed and insufficient accurate information has been provided.*

#### 4.2.1. Appraisal of mergers

*See section 3.2.4 (c) (merger control)*

62. Under the Merger Regulation,[102] authorities verify whether the concentration would trigger dynamics which could cause a 'significant impediment to effective competition'. If market power in the digital economy can be measured according to control of commercialisable personal information (see above 4.1.3), then merger decisions could in turn take account of the market effects of combining these capabilities.

63. So far the most significant Commission decision on a merger among undertakings in the digital economy concerned Google and DoubleClick.[103] The Commission, applying the threshold calculation criteria, determined that the merger lacked a Community dimension. The case was nevertheless examined by the Commission upon referral by parties to the concentration, it being capable of being reviewed under the national laws of several Member States.[104] Google was at the time reported to command a near monopoly of search in Europe,[105] and described the nature of its business as the provision of web search, as well as advertising.[106] The Commission however disregarded the search market, and rather considered Google's product market to be 'active mainly in the provision of online advertising space'. Analysing

[102] See footnote 73.
[103] See section 3.2.4 (c).
[104] Article 4 (5) of the Merger Regulation.
[105] See report of Search Engine Strategies conference, 13-15.02.2007. London, http://searchenginewatch.com/article/2066064/Stats-Show-Google-Dominates-the-International-Search-Landscape and compare with steady trend since then http://gs.statcounter.com/#search_engine-eu-monthly-200807-201402 (accessed 25.02.2014).
[106] See Google Inc. Annual Report 2008; http://investor.google.com/pdf/2008_google_annual_report.pdf . The Commission's market investigation did conclude however that other relevant markets were at least EEA-wide in scope. Brockhoff et al. According to Eurobarometer 299, only 7.4% of internet purchases are cross-border.

the extent to which the combination of the two undertakings' databases on customer search and web-browsing behaviour would affect competition in the relevant market, the Commission concluded that the combination would not create 'a competitive advantage in the advertisement business that could not be replicated by other players that have access to similar web-usage data.'

64. With such a purely economic approach to the case, the Commission did not consider how the merger could have affected the users whose data would be further processed by merging the two companies' datasets, conceivably to provide services, perhaps bundled or even tied to the simple search service, that were not envisaged when the data were originally submitted. The decision did not refer to consumer welfare nor to the users of Google's search engines, even though this potentially implicated every internet user in the EU. It therefore neglected the longer term impact on the welfare of millions of users in the event that the combined undertaking's information generated by search (Google) and browsing (DoubleClick) were later processed for incompatible purposes.

65. The Commission did analyse the effect on consumers, however, in two subsequent decisions concerning companies in the digital economy. Assessing the proposed acquisition of Tele Atlas (supplier of digital map databases) by TomTom (producer of portable navigation devices and supplier of GPS software), the Commission considered a theory of competitive harm and protection of client 'confidentiality', concluding that the merged entity would likely have incentives to mitigate any concerns which could lead to losing customers to competitors.[107] In the case of Microsoft's proposed purchase of Yahoo!'s internet search and search advertising businesses, the Commission considered Microsoft's increased ability, post-acquisition, to leverage its market power when negotiating distribution agreements, through for example bundling of products.[108] It concluded that potential for significant harm to users of Yahoo!'s internet search services was unlikely.

### 4.2.2. Access to markets and input by competitors

*See sections 3.1.3 (Legitimate and compatible purposes for data processing), 3.1.4 (consent and rights to information etc.), 3.2.4 (b) (abuse of market dominance) and 4.1.3 (measuring market power)*

66. In digital two-sided markets, such as the provision of multiple 'free' services in order to collect data coupled with the provision of online behavioural advertising space, marginal costs of supplying online services in a new market are low, and there is a distinct tendency towards tying of services (see paragraph 39). Powerful or dominant undertakings are able to exploit 'economies of aggregation'[109] and create barriers to entry through their control of huge personal datasets alongside proprietary software

[107] The Commission reasoned that in this case loss of confidentiality would could be considered as similar to product degradation which could lead to loss of customers to a rival which would not be compensated by any downstream gains; Commission Decision of 14/05/2008 declaring a concentration to be compatible with the common market and the EEA Agreement, Case No COMP/M.4854 - TOMTOM/ TELE ATLAS, C(2008) 1859. paragraphs 272-275.

[108] Commission Decision of 18.02.2010 (Case No COMP/M.5727- MICROSOFT/ YAHOO! SEARCH BUSINESS, C(2010), 1077.

[109] This term is explored in Bakos, Y. and Brynjolfsson, E., Bundling and Competition on the Internet, Marketing Science, Vol. 19, No. 1, Winter 2000, pp. 63–82. See also OECD Hearings on the Digital Economy, 2012; http://www.oecd.org/daf/competition/The-Digital-Economy-2012.pdf.

which organises the data. The information could in theory be considered an essential facility in a particular digital market (paragraph 40): the dominant undertaking has exclusive control of the information, while competitors lack the technical means to re-create the structure or system upon which the service relies. This effectively prevents entry to the market and restricts consumer choice for the 'free' services in question. At the same time, costs for the advertising market increase due to lack of competing offers.

67. Access to personal information could legally be granted to competitors on the basis of consent or other legitimate grounds**,** but this is a substantial hurdle under data protection law (see section 3.1.4). A dominant undertaking could thus seek to justify its refusal to supply competitors with datasets, including through exclusivity agreements, by claiming to adhere to data protection rules.

68. Such refusal to supply, it has been argued, may have an anti-competitive effect:[110] if there are limits on disclosure of datasets to competitors, the dominant undertaking could prevent the development of competing products from competitors. The undertaking could, therefore, try to 'shield' itself from remedies potentially imposed by competition authorities by claiming compliance with data protection rules. However, the dominant undertaking might still opportunistically infringe the data protection rules by using the dataset including personal data for a purpose incompatible with the one for which the data were originally collected in order to offer other services which competitors could never develop. In this context, there is clearly scope for cooperation between competition and data protection authorities in order to ensure that the respective rules are effectively enforced.

### 4.2.3. Data protection as a factor in consumer welfare

*See sections 3.2.4 (consumer welfare in competition law) and 3.3.2 (obligations of fairness and accurate information)*

69. According to a recent study,[111] consumers in the digital economy suffer discrimination partly due to lack of attention in the application of competition law. This neglect, according to the study, consists in the absence of uniform measures for reporting discriminatory practices and the lack of a harmonised approach to collective redress. While it is possible for consumer organisations to file a complaint before competition authorities, such claims are rare due to legal fees and low awareness of consumer rights.[112]

70. It should be borne in mind that consumers are also data subjects, whose welfare may be at risk where freedom of choice and control over one's own personal information is restricted by a dominant undertaking in the sorts of cases outlined above. Presenting

[110] Picker, R. C., 'Competition and privacy in Web 2.0 and the Cloud', Chicago John M. Olin Law & Economics Working Paper No. 414, June 2008, pp.13-14.

[111] 'Discrimination of Consumers in the Digital Single Market, study carried out by University of Osnabrück on behalf of European Parliament Directorate-General for Internal Polices Department for Economic and Scientific Policy, 2013.

[112] Panel on class actions, Competition Summit, Brussels, December 2013. In France the competition authority imposed heavy fines (EUR 27.6m and EUR 70m respectively) on two state-owned monopolies for infringements which included unfair use of client data; Décision n° 09-D-24 du 28 juillet 2009 relative à des pratiques mises en oeuvre par France Télécom sur différents marchés de services de communications électroniques fixes dans les DOM; Décision n° 12-D-25 du 18 décembre 2012 relative à des pratiques mises en œuvre dans le secteur du transport ferroviaire de marchandises.

offers to consumers as 'free', according to some psychological and behavioural economic research, is deceptive, blinds consumers to the actual costs which they will experience 'downstream' and distorts decision making, thereby harming both consumers and competition.[113]

71. Given the reach and dynamic growth in online services, it may therefore be necessary to develop a concept of consumer harm, particularly through violation of rights to data protection, for competition enforcement in digital sectors of the economy.

### 4.2.4. Remedies in competition decisions

*See sections 3.1.5, 3.2.5 and 3.1.3 (supervision etc.)*

72. Decisions on individual antitrust and merger cases typically impose remedies, including in one case a requirement for a company to sell a copy of a database which included personal information to one or several of its rivals.[114] Future remedies of this nature should be subject to strict conditions and safeguards in line with the principle of data minimisation (whereby only the personal information which is strictly necessary to perform a desired functionality should be collected).[115] In competition cases involving firms in the digital economy other remedial options could also be considered which address the harm to individuals' privacy. Options might include:

- offering users a paid service which minimised collection and retention of personal information;
- applying a proportionate limit to the retention of customer data,[116] for example along the lines of the 'compare and forget' method recommended by the Dutch data protection authority;[117]
- implementing data portability by giving the user options to withdraw their personal information and to port it to another service provider (see section 4.3.3); this would potentially empower individuals while also promoting competitive market structures; and
- placing strict controls on information processing across different parts of the business for incompatible purposes.

[113] Friedman, D.A., 'Free Offers: A New Look', 38 N.M. L. REV. 49, 68–69 (2008); Hoofnagle, C.J. and Whittington, J., 'Free: Accounting for the Costs of the Internet's Most Popular Price', 61 UCLA L. Rev. 606 (2014).

[114] Commission Decision of 19/02/2008 declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement Brussels, 19.02.2008, C (2008) 654 final (Case No COMP/M.4726 – Thomson Corporation/ Reuters Group.

[115] The data minimisation principle derives from Directive 95/46/EC Article 6.1(b) and (c).

[116] This solution was proposed by Bruno Lasserre, President of the French competition authority, 2013 Colloque New Frontiers of Antitrust, 22.02.2013.

[117] This recommendation was made in relation to the investigation into the whatsapp mobile communication application. The service provider could be allowed short-term read access to the full address book of a whatsapp user to help the user identify which of their contact persons were already whatsapp users. Once done, Whatsapp would then immediately delete the information; Dutch Data Protection Authority, 'Investigation into the processing of personal data for the 'whatsapp' mobile application by WhatsApp Inc.: Report on the definitive findings', January 2013.

### *4.3. Joined up enforcement to facilitate a 'race to the top' on privacy standards*

*See sections 3.1.4 (consent and right to information etc.), 3.2.4 (consumer welfare and competition law) and 3.3.2 (obligations of fairness and accurate information)*

*Application of competition and consumer protection law can be used as a tool to foster dynamic efficiency in digital markets and to encourage innovation. Recognition by the European authorities of the value of personal information in guidance and key decisions could foster privacy-enhancing services which serve the consumer's interest.*
*If companies are compelled to be transparent about the true value of the personal information which they collect, and market analyses take this value into account as part of competition decision, firms might begin to seek competitive advantages by reducing the periods over which information is retained or by providing a 'clear-my-data' button.*
*Competing firms that collaborate in the adoption of a certification scheme guaranteeing a high standard of privacy protection might be exempted from the prohibition of anticompetitive agreements, provided they fulfil the conditions of Article 101(3) TFEU*

#### 4.3.1. Fostering privacy as a competitive advantage

73. In certain markets, consumers may consider a more privacy-friendly service to be of better quality than a service which has an unclear or opaque privacy policy. In the provision of legal and medical services, private banking, security services, and exclusive luxury resorts, businesses typically compete on protecting privacy. It is reasonable to assume that, in such competitive markets, a failure by one company to respect data protection would damage their market power.[118] To a much more limited extent, some internet search services aim to differentiate on privacy.

74. Consumers who are used to enjoying free online services, however, may be willing to provide personal information in exchange for a free, quick and easy service, whether or not they are also aware of the accompanying risks. For such markets, more privacy-friendly terms may not automatically generate a consumer perception of superior quality.[119] Early research suggests that consumers could be willing to pay a premium for stronger privacy protection.[120] Firms operating in the digital economy do not yet consider privacy as opportunity for competitive advantage. On the contrary, there is the danger of a 'race to the bottom' of privacy protection, where failure to comply with data protection rules and the acquisition of data through anti-competitive means

[118] See EDPS Opinion on which stressed the desirability of promoting private enforcement of data protection principles through competition in privacy-compliant products and services as a means of expanding its position and better addressing the expectations of privacy-aware consumers. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-07-25_Dir95-46_EN.pdf

[119] According to (inconclusive) results of recent research, 'when consumers have to balance a trade-off between shopping from a privacy-friendly, or a cheaper firm, the latter attracts the overwhelming majority'; Preibusch, S., Kuebler, D. and Beresford, A., R., 'Price versus privacy: an experiment into the competitive advantage of collecting less personal information', published online 07.08.2013.

[120] Tsai, J. Y., Egelman, S., Cranor, L. and Acquisti, A., 'The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study', Information Systems Research, Vol. 22 (2), June 2011, pp. 254 – 268.

may have become symptomatic of market power, with externality costs borne by users.[121]

75. A useful comparison may be drawn with the spread in the 1960s and 1970s of the notion of corporate social and environmental responsibility. Companies began to realise the importance of the socio-economic impact of their business and how it was perceived by their customers. They now typically benchmark their own policies against those of competitors, and there is a genuine market for product safety and green technologies. A more joined-up approach to data protection and competition could help stimulate a similar level of competition in online services.

### 4.3.2. Consumer choice, consent and transparency

76. Choice depends on the availability of competing services and the consumer's ability to understand the information provided about those services.[122] Confronted by multi-service companies in the digital economy, there are several significant obstacles to genuine choice. If personal information is collected as a condition for using one particular service, and then processed by the same company for the purposes of another service, it is already difficult for users to predict what will be done with their data.[123]

77. This difficulty is compounded by lengthy 'privacy policies': a study has calculated that it would take on average each internet user 244 hours per year to read the privacy policy belonging to each website they view, which is more than 50% of the time that average user spends on the internet.[124] These policies typically contain statements about the future use of data which are concealed in legal small print or which require decoding due to vague, elastic terms like 'improving customer experience'.[125]

78. Moreover, with average smart phone users downloading 37 apps for purposes ranging from gaming to banking, only 61% of most popular apps have a privacy policy.[126]

---

[121] See for example Grunes, A.P., 'Another look at privacy', Geo.Mason L. Rev Vol 20:4, p.1112; Jones Harbour, P., J., and Koslov, T., I., Section 2 in a Web 2.0 world: An expanded vision of relevant product markets, Antitrust Law Journal, Vol. 76 (2010), pp.769-797.

[122] Article 11 of the proposed data protection regulation provides for data protection policies which are 'transparent and easily accessible'.

[123] See letter from Article 29 Working Party to Google Inc. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121016_letter_to_google_en.pdf (accessed 10.03.2014).

[124] McDonald, A. M. and Cranor, L. F., 'The Cost of Reading Privacy Policies', A Journal of Law and Policy for the Information Society 2008, Privacy Year in Review, p.17.

[125] The term 'privacy policy' may itself be deceptive, as extensive research carried out in the US indicates. According to one survey of US internet users, under half of respondents found privacy policies easy to understand, of whom two-thirds believed (incorrectly) that sites with a privacy policy would not share data; Turow, J., Americans and Online Privacy: The System is Broken, June 2003. A clear majority of the privacy policies in the Fortune 500 Study were assessed as written at a level that surpasses the reading ability of the average U.S. adult; Shannon Wheatman1 & Michelle Ghiselli Privacy Policies: How to Effectively Communicate with Consumers and Avoid Judicial and Regulatory Scrutiny'. The FTC has found that most corporate privacy policies are 'incomprehensible' and that 'privacy policies do a poor job of informing consumers about companies' data practices or disclosing changes to their practices;' Preliminary Staff Report: 'Protecting Consumer Privacy in an Era of Rapid Change,' March 2012. In March 2014, a French consumers group launched legal action against three of the largest social networks on grounds of breach of both consumer and data protection rules, having previously criticised the service providers for confusing ('*elliptique et pléthorique*') contractual terms; http://www.quechoisir.org/telecom-multimedia/internet/editorial-donnees-personnelles-main-basse-sur-la-vie-privee (accessed 25.03.2014).

[126] Article 29 Working Party Opinion 02/2013 on apps on smart devices, WP 202, 27.02.2013.

This creates an asymmetry of knowledge which invokes the obligations of traders to provide clear and unambiguous information under EU consumer protection law, and calls into question whether data subjects have sufficient information to give informed consent to data processing.[127] The situation is likely to be compounded by the growth of the Internet of Things, which will include many technical or embedded devices collecting personal data, with the result that their users will be unable to consult the privacy policy on the device itself, but would have to find paper documentation or more likely browse from another device to the relevant web sites.

79. Successful online providers persuade increasing numbers of customers to provide more personal information which increases the value of the service to advertisers, thus generating 'network effects' whereby yet more customers are attracted to the service.[128] In the case of 'free' online services, customers may not be offered an alternative version of a provider's offering in which personal information are not to be used for marketing purposes. Customers have limited room, if any, to negotiate the terms and conditions of use, representing a 'significant imbalance' between provider and user which could also trigger investigation into the legality of data processing. This calls into question the existence of a genuine choice under Article 7(a) of the Data Protection Directive and in turn the validity of consent to processing of personal information. Where there is a limited number of operators or when one operator is dominant, the concept of consent becomes more and more illusory.[129]

80. There have therefore been calls for the responsibility to protect personal information to shift more visibly from the user to the service provider, as with consumer protection rules (see section 3.3.2).[130] One response to these challenges could be to consider standards for transparency and intelligibility of contractual terms in online services. Organisations could be required to reveal more about their decision making in data processing operations.[131] A transaction cost economics approach has also been recommended, which takes into account contextual factors in assessing the value of products and services which are promoted as free but which incur 'myriad, hidden,

[127] In an order on the defendants motion to dismiss a class action complaint which alleges that the scanning of user emails amounts to a breach of US wiretap laws, a US district court found 'a reasonable Gmail user who read the Privacy Policies would not have necessarily understood that her emails were being intercepted to create user profiles or to provide targeted advertisements,' nor that 'non-Gmail users who are not subject to Google's Privacy Policies or Terms of Service have impliedly consented to Google's interception of their emails to Gmail users;' United States District Court Northern District of California San Jose Division, Case No.: 13-MD-02430-LHK, Order Granting in Part and Denying in Part Defendant's Motion to Dismiss, 11.07.2013, pp.26-28.

[128] Network effects occur where the utility of a service increases the more people use it, meaning that entrants require a 'critical mass' of users in order to compete, while users may only use the competing service (e.g. a computer operating system) when it has been generally adopted. See Grunes, A. P. (2013), Another Look at Privacy (August 13, 2013), George Mason Law Review, Vol. 20, No. 4, 2013, p. 1120.

[129] Coates (2011).

[130] 'In the context of online privacy, this implies emphasis should be placed less on notice and choice and more on implementing policy decisions with respect to the utility of given business practices and on organizational compliance with fair information principles (FIPs). In other words, the focal point for privacy should shift from users to (a) policymakers or self-regulatory leaders to determine the contours of accepted practices; and (b) businesses to handle information fairly and responsibly.' See in this context also the Article 29 Working Party's Opinion on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (April 2014) and the increasing emphasis on the principle of accountability for controllers.

[131] Tene, O and Polonetsky, J.(2013), 'Big Data for All: Privacy and User Control in the Age of Analytics', 11 Nw. J. Tech. & Intell. Prop. 2.239 (2013).

non-pecuniary costs,' so that all parties have a more equal level of understanding of the value of the personal information which is being gathered and processed.[132]

81. The enforcement of competition rules requires an evaluation of whether consumers regard different services as being substitutable. It follows that this analysis should pay regard to transparency and the ultimate cost to consumers of privacy policies, and to whether the choice is genuine, and whether consent to information processing is valid.

### 4.3.3. Control of one's own information

82. Better informed consumers should be better able to choose between competing online services. They should be able to withdraw and to transfer data which record their activities and are stored in the cloud, whether in the context of social networks, search engines, online banking, energy consumption, medical or fitness tracking applications. As a Commission competition expert has noted, 'the harder it is for an individual to move [his/her] data, the stronger will be the position of the provider that controls that data, and the more difficult it will be for new entrants to succeed.'[133]

83. Data portability (paragraph 26) could release synergies between competition law and data protection law in at least two ways. [134] First, it could prevent abuse of dominance, whether exclusionary or exploitative, and consumers being locked into certain services through the limitation of production, markets or technical development to the prejudice of consumers.[135] It would emulate the benefits of number portability provided for in telecommunications law.[136] Second, data portability could empower consumers to take advantage of value-added services from third parties while facilitating greater access to the market by competitors, for example through the use of product comparison sites or of companies offering energy advice based on smart metering data.[137]

## *4.4. Supervision and enforcement*

*See sections 3.1.5, 3.2.5 and 3.1.3 (supervision etc.)*

84. Separate consistency arrangements in the EU already exist for the regulation of competition, consumer protection and data protection through, respectively, the European Competition Network, the Consumer Protection Cooperation Network and the Article 29 Working Party. The distinctness and independence of these authorities must continue to be fully respected. However, given the challenges set out in this

[132] Hoofnagle and Whittington (2014).
[133] Coates, K., *Competition Law and Regulation of Technology Markets*, 2011.
[134] Article 18 of the proposed General Data Protection Regulation; COM (2012) 11 final. There are already public-private initiatives in several Member States which enable individuals to access directly their own data which are held by companies and to choose to transfer them to competing providers. See for example in the UK http://www.midatalab.org.uk/ and France http://mesinfos.fing.org/ .
[135] Article 102(2)(b) of TFEU. See also Mantelero, A., 'Competitive value of data protection: the impact of data protection regulation on online behaviour', International Data Privacy Law, 2013, Vol. 3, No. 4, pp. 229-238.
[136] Article 30, Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), OJ L 108, 24.04.2002.
[137] 'Allowing data subjects/customers to have direct access to their data in a portable, user-friendly and machine-readable format may help empower them, and redress the economic imbalance between large corporations on the one hand and data subjects/consumers on the other. It would also let individuals "share the wealth" created by big data and incentivise developers to offer additional features and applications to their users;' Article 29 Working Party, Opinion 03/2013 on purpose limitation.

document, it may be sensible for the Commission and the EDPS at EU level together with national competition, consumer protection and data protection authorities to agree upon a more holistic approach to enforcement. This would be especially timely in the light of the review of consumer protection cooperation and ongoing negotiations on the data protection regulation, which includes provisions on a consistency mechanism. Dialogue between authorities at these two levels – European and national - could become more systematic wherever a specific case arises in which consumer welfare and data protection concerns appear to be at stake.

## 5. Conclusion: further investigation and discussion required

*The rapidly expanding online market or markets… increasingly touch all aspects of business. Making sure competition works effectively in these markets will be a major priority… the growing collection, processing and use of consumer transaction data for commercial ends …is proving an increasingly important source of competitive advantage [which could be] an increasing source of consumer detriment.*

From Beesley Lectures speech by David Currie, chairman of UK Competition and Markets Authority, 7.11.2013.

85. This preliminary Opinion has explored and considered the possible convergences and tensions between three areas of EU law, against the fast evolving backdrop of big data. Although privacy and the protection of personal data are public interests and fundamental rights recognised in the Treaties, the lack of interaction in the development of policies on competition, consumer protection and data protection may have reduced both the effectiveness of competition rules' enforcement and the incentive for developing services which enhance privacy and minimise potential for harm to the consumer. In the digital economy personal information represents a significant intangible asset in value creation and a currency in the exchange of online services. This has potentially far-reaching implications for the interpretation of key concepts including transparency, market dominance, and consumer welfare and harm.

86. A comprehensive response to these challenges requires more time for investigation, reflection and discussion, but might include any or all of the following:

- **raised awareness** among consumers, service providers and regulators of current and future technological developments in relevant markets in the digital economy and the implications for competitiveness, consumer welfare and choice and innovation around privacy-enhancing services;

- **effective guidance** on the application of privacy, competition and consumer protection rules for online services, in particular those promoted as 'free' services, which takes into account the views of customers and competitors and evidence of customer preferences and concerns;

- **cooperation** between authorities in investigation and enforcement, for example in identifying scenarios and possible standards for measuring market power in the digital economy, and consultation on investigations into individual cases; and

- **a review of competition legislation** for 21st century digital markets, including its interfaces with other areas of law and possibilities for productive interaction with other relevant authorities.

87. Personal information has prompted and sustained growth in the digital economy. Individual consumers should be able to enjoy a fairer share of the fruits of that growth. Competition and data protection authorities are increasingly recognising this as a pivotal challenge in building trust and accountability across the digital economy. Data protection presents a unique opportunity to give individuals the tools to protect themselves and to make the enforcement of competition and consumer protection rules more effective.

88. The next step is to explore the scope for closer coordination between regulators to achieve these aims. This coordination should not be restricted to Europe but rather reflect the global reach of companies in the digital economy. The EDPS looks forward to facilitating this discussion.

Done in Brussels, 26 March 2014

(**signed**)

Peter HUSTINX
European Data Protection Supervisor

EUROPEAN DATA PROTECTION SUPERVISOR

# *Annex: Data protection, competition and consumer protection in the EU: A comparative overview*

| | ***Data protection*** | ***Competition law*** | ***Consumer protection*** | ***Interfaces in digital economy*** |
|---|---|---|---|---|
| ***Legal framework*** | ➢ *CFR Arts. 7 and 8*<br>➢ *TFEU 16* | ➢ *TFEU 101-106* | ➢ *CFR 38*<br>➢ *TFEU Arts. 12 and 169* | ➢ *Core EU values and economic mission* |
| ***Relevant secondary legislation*** | ➢ *Directive 95/46/95*<br>➢ *Regulation (EC) No 45/2001*<br>➢ *Directive 2002/58/EC*<br>➢ *General Data Protection Regulation (under negotiation)* | ➢ *Regulation 1/2003 (Modernisation)*<br>➢ *Regulation 139/2004 (Mergers)* | ➢ *Directive 93/13/EEC (unfair contract terms)*<br>➢ *Directive 98/6/EC (price indication)*<br>➢ *Council Directive 2005/29/EC (unfair commercial practices)*<br>➢ *Directive 2006/114/EC (misleading advertising)*<br>➢ *Regulation 2006/2004 (cooperation between authorities)*<br>➢ *Directive 2011/83/EU (Consumer Rights)* | ➢ *Rules for promoting sound functioning of the internal market.*<br>➢ *Rules for ensuring protection of individual consumers* |
| ***Scope of application*** | ➢ *All data controllers established in the EU or using equipment situated in the EU. Provisions scalable according to the nature and volume of data processed.*<br>➢ *(To be extended under GDPR to cover any data controller offering goods or services to or monitoring* | ➢ *Any economic activity which 'may affect trade between Member States.'*<br>➢ *Dominant undertakings have 'special responsibility' to avoid distortions to* | ➢ *All goods and services supplied or consumed in the internal market.* | ➢ *Impact on individuals in the EU of economic activity which concerns the internal market* |

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax: 02-283 19 50

| | ***Data protection*** | ***Competition law*** | ***Consumer protection*** | ***Interfaces in digital economy*** |
|---|---|---|---|---|
| | *behaviour of data subjects residing in the EU)* | *competition.* | | |
| ***Data control and relevant markets*** | ➢ *Compatible purposes for data processing* | ➢ *Definition of relevant market and substitutability of products and services* | | ➢ *Defining relevant markets fuelled by personal data*<br>➢ *Measuring digital market power* |
| ***Transparency and choice*** | ➢ *Rights to information and to access data in an intelligible form*<br>➢ *Freely-given, specific, informed and unambiguous consent*<br>➢ *Right to data portability* | ➢ *Tying and bundling of services*<br>➢ *Preventing competition through refusal to supply an essential facility* | ➢ *Clear and intelligible information on prices and products* | ➢ *Common understanding of value of personal data*<br>➢ *Ownership of own data through exercising data portability* |
| ***Prevention of harm*** | ➢ *Data minimisation*<br>➢ *Confidentiality and security of processing* | ➢ *Notion of consumer welfare*<br>➢ *Exploitative pricing of services*<br>➢ *Theory of harm to consumers in mergers*<br>➢ *Exemptions to state aid rules* | ➢ *Notion of 'good faith' in contracts*<br>➢ *Prohibition of misleading claims about products and services* | ➢ *Data protection a factor of consumer welfare*<br>➢ *Use of privacy-promoting remedies in competition decisions*<br>➢ *Allowing competitors to collaborate on developing privacy-enhancing services* |
| ***Supervision, enforcement, sanctions remedies*** | ➢ *Independent national authorities*<br>➢ *EU wide cooperation through Article 29 Working Party and (under negotiation) consistency mechanism*<br>➢ *Right to a judicial remedy for violation of rights*<br>➢ *Right to receive compensation*<br>➢ *Administrative sanctions as a proportion of a company's annual turnover (under negotiation)* | ➢ *Enforcement through national competition authorities and the Commission for the EU*<br>➢ *Authorities cooperate through European Competition Network*<br>➢ *Sanctions for infringement of anti-competitive agreements of up to 10% of total turnover* | ➢ *National authorities only*<br>➢ *CPC Network identifies common enforcement priorities each year with coordinated compliance checks and sector specific projects*<br>➢ *No common EU approach to investigation of breaches of consumer law except for 'intra-Community infringements'* | ➢ *Dialogue and cooperation on cases where competition, consumer welfare and data protection concerns overlap.* |

| | ***Data protection*** | ***Competition law*** | ***Consumer protection*** | ***Interfaces in digital economy*** |
|---|---|---|---|---|
| | | ➢ *No harmonisation of rights to judicial remedy for consumers* | ➢ *Rare for authorities to secure compensation for breaches of consumer law* | |

***Abbreviations:***

***CFR: Charter of Fundamental Rights of the European Union***

***TFEU: Treaty on the Functioning of the European Union***