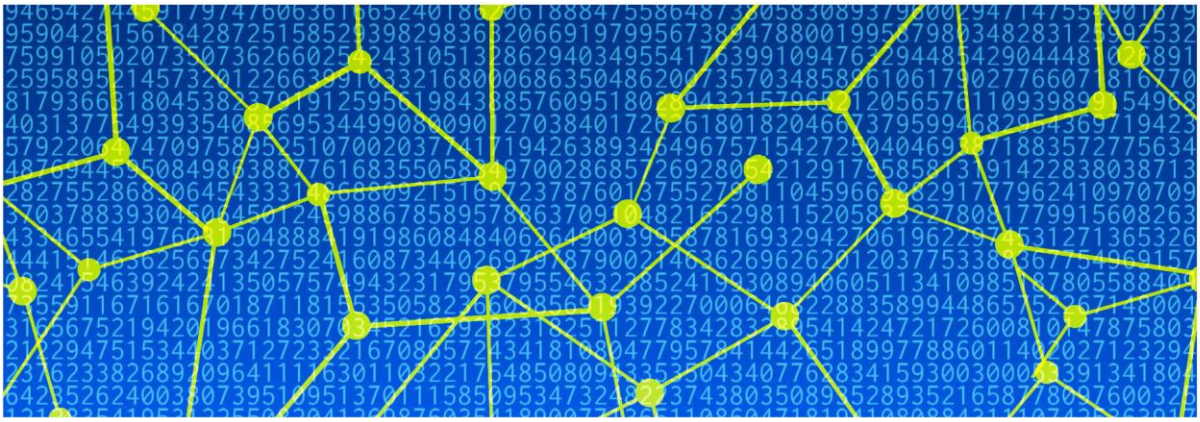

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 8/2016

EDPS Opinion on coherent enforcement of fundamental rights in the age of big data

EDPS

23 September 2016

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion relates to the EDPS' mission to advise the EU institutions on the data protection implications of their policies and foster accountable policymaking - in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'.

Executive Summary

Processing personal information is indispensable to web-based services. The EU's Digital Single Market Strategy recognises the potential of data-driven technologies and services as a catalyst for economic growth. Such services over the Internet have become dependent on often covert tracking of individuals, who are generally unaware of the nature and extent of that tracking. Dominant companies in these markets may be able to foreclose new entrants from competing on factors which could benefit the rights and interests of individuals, and may impose unfair terms and conditions which abusively exploit consumers. An apparent growing imbalance between web-based service providers and consumers may diminish choice, innovation and the quality of safeguards for privacy. This imbalance may also raise the effective price - in terms of personal data disclosure - far beyond what might be expected in fully competitive markets.

In 2014 the EDPS issued a Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data. We observed a tendency, despite obvious synergies like transparency, accountability, choice and general welfare, for EU rules on data protection, consumer protection and antitrust enforcement and merger control to be applied in silos. We therefore launched a debate on how the EU's objectives and standards might be applied more holistically. This new Opinion argues that the Digital Single Market Strategy presents an opportunity for a coherent approach, and updates the 2014 Preliminary Opinion with some practical recommendations to the EU institutions on how to remedy the situation. It addresses the mounting concern that concentration in digital markets could harm the interests of individuals as data subjects and consumers.

The EU institutions and bodies, and national authorities when implementing EU law, are required to uphold the rights and freedoms set out in the Charter of Fundamental Rights of the EU. Several of these provisions, including the rights to privacy and to the protection of personal data, freedom of expression and non-discrimination, are threatened by normative behaviour and standards that now prevail in cyberspace. The EU already has sufficient tools available for addressing market distortions that act against the interests of the individual and society in general. A number of practices in digital markets may infringe two or more applicable legal frameworks, each of which is underpinned by the notion of 'fairness'. Like several studies in recent months, we are calling for more dialogue, lesson-learning and even collaboration between regulators of conduct in the digital environment. We also stress the need for the EU to create conditions online, as well as offline, in which the rights and freedoms of the Charter may thrive.

This Opinion therefore recommends establishing an Digital Clearing House for enforcement in the EU digital sector, a voluntary network of regulatory bodies to share information, voluntarily and within the bounds of their respective competences, about possible abuses in the digital ecosystem and the most effective way of tackling them. This should be supplemented by guidance on how regulators could coherently apply rules protecting the individual. We also recommend that the EU institutions with external experts explore the creation of a common area, a space on the web where, in line with the Charter, individuals are able to interact without being tracked. Finally, we recommend updating the rules on how authorities apply merger controls better to protect online privacy, personal information and freedom of expression.

TABLE OF CONTENTS

I. OPENING UP THE DEBATE 5

1. BACKGROUND AND STRUCTURE OF THIS OPINION 5
2. MOVING FROM ANALYSIS TO ACTION 5
3. STRATEGIC IMPORTANCE OF THIS ISSUE FOR DATA PROTECTION AUTHORITIES 5
4. THE 'VALUE' OF PERSONAL DATA IN DIGITAL MARKETS 6

II. POWER AND ACCOUNTABILITY 7

1. SCALABLE LEGAL OBLIGATIONS 7
2. CONCENTRATION OF MARKET AND INFORMATIONAL POWER 7

III. SYNERGIES READY TO BE EXPLOITED 8

1. COMMON GOALS BUT LIMITED COOPERATION 8
2. SEPARATE BUT RELATED JURISDICTIONS 9
3. OPPORTUNITIES FOR WORKING TOGETHER 10

IV. FOSTERING PRIVACY AND PRIVACY-ENHANCING TECHNOLOGIES AS A COMPETITIVE ADVANTAGE 12

1. TRUST AND TRACKING 12
2. PRIVACY AS A FACTOR OF QUALITY, AND DETERMING THE TRUE PRICE OF 'FREE' SERVICES 13
3. IMBALANCES WITHIN THE DIGITAL TRANSACTION 13
4. WEAK MARKET FOR PRIVACY-FRIENDLY SERVICES 13

V. RECOMMENDATIONS: SHAPING AN EU CYBERSPACE BASED ON EU VALUES 14

1. BETTER REFLECT THE INTERESTS OF THE INDIVIDUAL IN BIG DATA MERGERS 14
2. A DIGITAL ENFORCEMENT CLEARING HOUSE 15
3. AN EU VALUES-BASED COMMON AREA ON THE WEB 16

VI. CONCLUSION 16

Notes 18

I. OPENING UP THE DEBATE

1. Background and structure of this Opinion

Our 2014 Preliminary Opinion on 'Privacy and Competitiveness in the Age of Big Data' (hereafter, 'the Preliminary Opinion') compared EU legal frameworks for data protection, competition and consumers, and concluded that there were some obvious synergies in the context of digital markets[1]. We made some tentative recommendations for EU institutions that were refined following a workshop hosted by EDPS in June 2014[2], including:

1. to understand better **the 'value' of personal data in digital markets** and review approaches to market analysis, in particular for those web-based services promoted as 'free', with retrospective or ex-post analysis of the impact of enforcement decisions;

2. to consider how to **foster privacy-enhancing technologies as a competitive advantage**;

3. to review **EU legislation and relevance for 21st century digital markets**;

4. to consider practical steps for **cooperation between authorities**, including closer dialogue and joint investigations.

2. Moving from analysis to action

This Opinion follows up on these issues, but also responds to a debate which, since 2014, has moved from more abstract legal arguments to more urgent concerns. Concentration and monopoly power, particularly in digital markets, pose problems for not only competitiveness but also for privacy and freedom of expression. The Digital Single Market Strategy adopted by the European Commission in May 2015 stated an intention to achieve a level of harmonisation of rules in the digital ecosystem and to make Europe a leader in the global digital economy[3]. The strategy depicted the data economy as crucial for enhancing EU competitiveness, while data were defined as 'a catalyst for the economic growth'. This Opinion is the latest output of the EDPS's ongoing engagement with this wide ranging strategy[4]. It aims to go beyond legal commentary by pointing to practical measures to address these enforcement challenges in a coherent way[5].

3. Strategic importance of this issue for data protection authorities

The interface between competition and privacy should be a central, strategic and long-term concern for all independent data protection authorities. Personal data have played a central role in the evolution of digital markets, some of which can now be considered essential services. As we have previously argued[6], the rapid development of personal-data driven technologies and data processing operations enabled by those technologies, such as Big Data and the Internet of Things, place the right to data protection as well as several other fundamental rights under unprecedented strains. Certain classic fundamental rights laid down in the Charter - the right to privacy (Article 7), to freedom of expression (Article 11) and to non-discrimination (Article 21) - were conceived originally as protections against interference by the state. However, it is now clear that in the digital age safeguards are equally required against potential interference by non-state entities and individuals, leading (among other things) to the right to data protection enshrined in Article 8 of the Charter. Most recently, the UN Special Rapporteur on freedom of expression calling on information communications and technology sector to respect human rights[7].

Network effects, the Commission has found, are a characteristic of digital markets[8]. The social and professional costs of opting out of many web-based services has increased, with a lack of interoperability and the available choices offering often only low-level privacy protections. One parameter of competition is choice, but it is now virtually impossible to choose not to be tracked while consuming digital services[9]. The apparent splintering of the web according to state boundaries and the segregation of the individual's online experience into a limited number of 'walled gardens' threatens privacy, personal information, freedom of expression and freedom to innovate amid concentration of profit and market power.

Meanwhile unfair price discrimination - by exploiting differences in consumers' identifiable sensitiveness to price - could lead to extraction of consumer surplus and increase in profits[10]. Recent studies have pointed to the potential in the future of machine-learning algorithms to achieve perfect first degree price discrimination, with firms segmenting the market into each individual consumer and charging him according to his willingness to pay. In the near future, technology could potentially enable tacit collusion between companies in digital markets to fix prices through data and self-learning algorithms[11]. This could lead, in economic terms, to maximum revenue but no consumer welfare, with obvious negative implications for fundamental rights. Data protection and other competent authorities will need to be vigilant.

4. The 'value' of personal data in digital markets

Much debate since 2014 has focused on the 'value' of Big Data and the extent to which it may be equated with personal data. While many big data applications are concerned with factual data, like the weather or machine processes, businesses and governments are increasingly using massive volumes of personal information to understand, predict and shape human behaviour[12]. The largest web-based service providers, which include several of the top ten biggest companies in the world, owe their success to the quantity and quality of personal data under their control as well as to the intellectual property required to analyse and to extract value from these data[13]. Personal information has become a factor of competition for companies, described as a 'raw material for digital business models', used to improve products and targeted advertising[14].

It is now commonplace for personal information to be compared to a currency used to gain access to online services, and the Commission proposal on digital contracts even recognises that personal data may be used as payment[15]. Data may be a directly-traded commodity, or it may have an ancillary function as an input for the creation of individual user profiles[16]. 'Multisided' digital platforms, which are typical mediators for most people's online experience, treat individuals and organisations as suppliers of ideas and products to be matched with others. Successful data-driven multi-sided platforms have grown through offering 'free' content and/or services in order to gather masses of personal information, revealing individuals' past, present and even future habits and preferences. The platforms attract paying customers on one side – typically advertisers – through the collection and analysis of personal information gathered from non-paying customers on the other side.This blurs the traditional distinction between consumer and producer[17].

Commercial control of data could be the missing element which explains the remarkable inflation in market value of successful companies in the digital sector[18]. Our Preliminary Opinion cited then European Commission Vice President Almunia's statement that there had yet to be a full sector analysis of free digital services[19]. Competition authorities where defining relevant markets and quantifying market power in specific cases have tended to focus on the 'paying' side – which until now has typically equated to those seeking advertising opportunities. Meanwhile the other side 'non-paying' side has not been pursued on the grounds that it is hard to quantify and is rather a concern for other areas of law. The efficiency of these markets has been called into question because of the asymmetry of information between the sides of the

market[20]. Given this uncertainty we welcome the openness of the European Commissioner for Competition to consider the role of data, and not simply company turnover, in merger control cases[21].

In the EU, personal information cannot be conceived as a mere economic asset[22]: according to the case law of the European Court of Human Rights, the processing of personal data requires protection to ensure a person's enjoyment of the right to respect for private life and freedom of expression and association[23]. Furthermore, Article 8 of the EU Charter and Article 16 of the Treaty on the Functioning of the European Union (TFEU) have specifically enshrined the right to the protection of personal data. In consequence, the 2016 General Data Protection Regulation contains specific safeguards that could help remedy market imbalances in the digital sector: Data protection authorities need to enforce data minimisation, which requires personal information only to be processed where 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'[24], and the right of individuals to receive information regarding the logic involved in the automated decision-making and profiling[25]. Data protection and consumer enforcement should also be ready and able to inform and to advise competition authorities on merger cases in the digital sector where there is reason to be believe the deal could harm individuals.

II. POWER AND ACCOUNTABILITY

1. Scalable legal obligations

Data protection, privacy (confidentiality of communications) and consumer laws have recently been or are being revised to safeguard individuals' rights more effectively in the new digital reality[26]. One of the most important novelties of the new General Data Protection Regulation is the integration of the principle of accountability, something well established in competition law but relatively new to data protection law. According to this principle, organisations subject to data protection obligations are expected to be able to demonstrate that necessary steps have been taken to ensure compliance with the rules, with data protection authorities intervening only to check, in particular, when there is an indication of a breach. Obligations in each of these areas are scalable: where a company, for example, enjoys greater market power (a concern for competition authorities), or a stronger contractual position (consumer protection), or is responsible for riskier data processing operations (data protection), they are required to be more diligent in the steps they take to comply.

However, as we have argued in recent Opinions, effective laws while necessary are not sufficient for creating a culture of accountability, including in markets where behaviour may be harming individuals and society as a whole, and where there is ever more concentration of market power. Regulation tends to lag behind technology and markets; innovative and dynamic services emerge which disrupt established industries by more efficiently satisfying the demands of consumers. Often the application of rules to these ground-breaking services is contested and requires clarification from the courts[27].

2. Concentration of market and informational power

At the EDPS workshop in 2014 it was argued that 'economies of scope' and concentration in 'big data' related markets could culminate in 'winner-takes-all' situations and near monopolies which enjoy increasing returns to scale due to the absolute 'permanence' of their digital assets[28]. Concentrations in digital markets over recent years have reduced competition for many services, with the biggest companies now established in their dominance for over a decade, belying the reputed transitory character of these markets. Traditional approaches are considered

to be failing to keep profits to normal levels resulting in excessive prices to consumers[29]: according to the few ex-post merger reviews that have been conducted, most mergers tend to lead to price increases[30]. Although dominant companies in digital markets owe their success to the quality of their products, in general concentrations seem likely over time to increase price and profits, diminish quality of service and innovation.

The biggest companies in the digital sector have significant power over communications and control over gateways to the Internet, even if authorities may lack a means for determining their 'market power' in a traditional sense[31]. A majority of people now access news on social media, and web-based service algorithms determine the content to be served to individual users according to their profile, with growing concerns that the online experience could be filtered and become a series of echo chambers[32]. Similarly, concentrations in digital markets are unlikely to reinforce the principle in EU law of data minimisation – something that might be considered a sort of efficiency in the volume of personal data being processed. Instead, concentrations have led to the gathering and combination of more personal data, with no visible improvement in the transparency of data use policies.

Concerns about monopoly power and informational power are thus converging in a manner analogous to the end of the 19th century when both antitrust and human rights became major public policy concerns in Europe and the United States. Powerful organisations have the potential to diminish the quality of privacy and freedom enjoyed by consumers of digital services, or to act as effective censors of online content, even if they do not yet fully exercise that power[33]. Since we published our Preliminary Opinion, policymakers are paying greater attention to the nature of digital transactions requiring not money payment but the disclosure of personal information, especially where personal data processing is not technically necessary for the provision of the service[34].

III. SYNERGIES READY TO BE EXPLOITED

1. Common goals but limited cooperation

Data protection, competition and consumer law in the EU all aim, as we have noted, to protect and to promote welfare and to help create a single European market[35]. Ongoing dialogue over the past two years has highlighted in particular the notion of fairness pervading each of these fields and enshrined in the relevant articles of the EU Charter and the TFEU:

- fairness is perhaps the most fundamental criterion for lawful trading practices in consumer law;
- fairness of personal data processing is a core principle alongside lawfulness and transparency;
- competition law makes concessions to anti-competitive agreements 'allowing consumers a fair share' of the benefit and includes in its definition of abuse of dominance 'imposing unfair purchase or selling prices'[36].

Despite this, cooperation between authorities at European level continues to be limited[37]. In our Preliminary Opinion we discussed the common concern for the consumer. However, the notion of 'consumer welfare' in competition law has never been clearly defined, and it has tended to be used to address market structure and economic efficiency and only indirectly addresses individual consumer concerns, such as privacy[38]. TFEU Article 102 prohibits abuse of dominance in the form of 'unfair purchase or selling prices or other unfair trading conditions':

yet competition authorities tend to leave action against such exploitative conduct to consumer enforcement, while sometimes consumer enforcers in turn leave unfair consumer terms cases to data protection authorities[39].

Some interaction between authorities at national level has delivered results, for example:

- according to an interim decision in September 2014 of the French competition authority, GDF Suez had abused its dominant position by using personal data collected when it was a state monopoly to promote a gas and electricity package to an open unregulated market. The authority instructed GDF to disclose part of its customer database to competitors after giving the individuals the chance to opt out of the disclosure;

- the UK data protection authority advised the UK competition authority in August 2015 on their proposal to invite households who had not switched energy suppliers for three years or more to opt out of having their details shared with rival suppliers;

- in September 2015 the Belgian competition authority imposed a fine of €1.9 million on the Belgian National Lottery for using the personal data also acquired as a public monopoly for the incompatible purpose of marketing a commercial betting service "Scooore!" on the adjacent market of sports betting. The authority considered this to be an abuse of dominance in using information which could not be replicated by its competitors;

- in 2016, an investigation was launched by the *Bundeskartellamt* into privacy policies applied by the allegedly dominant social media company Facebook, having had close contact with data protection authorities, consumer protection associations and other national competition authorities[40].

Nevertheless, overall there is a quite fragmented scenario in enforcing EU rules, with competent authorities not necessarily talking to each other whilst dealing with cases featured by considerable overlaps in terms of substance. For example, joint meetings of the Article 29 Working Party, the European Competition Network and the Consumer Protection Cooperation Network, the respective EU-level coordination bodies, would be useful.

2. Separate but related jurisdictions

Regulators are often under great pressure to meet public expectations within limited resources and growing workload and it is natural to focus on their own competences. The boundaries of the respective powers and competences of the bodies must be respected: clearly authorities should not, and probably cannot, enforce laws in other legal areas[41]. No single area of law is a panacea for all problems and it would be inappropriate for one area of regulation to look to another area to compensate for its own weaknesses. Authorities in each area have limited tools at their disposal, for example competition enforcement can only address abuse of dominance, cartel behaviour and mergers which are not in the consumer interest; abusive conditions of service are not necessarily an antitrust issue.

An important merger case subsequent to our Preliminary Opinion concerned the acquisition of WhatsApp – a popular messaging app which scans entire address books but does not market the user information – by Facebook - which has a very different data use approach. The US Federal Trade Commission required the parties to give customers notice and choice if they departed from the conditions. The European Commission, acting as the EU competition authority, determined that there was no basis in the Merger Regulation to require the acquiring entity to respect the privacy agreement signed up to by WhatsApp customers[42]. Each approach however implied that users of the messaging services were required to accept the new

conditions or to be barred from using the services. Recently a change to the privacy terms of the WhatsApp messaging service has led the Competition Commissioner to ask questions of the merged entity[43]. In the case of future mergers of a similar nature, individuals might benefit from a more coherent response from competition, consumer and data protection authorities. Supervisory authorities must be fully equipped to anticipate and to prevent both behaviour and concentrations that could be harmful for the individual.

None of these regulatory jurisdictions is hermetically sealed from the others. High concentration in markets could undermine the protection of those fundamental rights, even in cases where no anticompetitive conduct is assessed by antitrust enforcers. Authorities already are expected, according to case law, to consider the likely incentives for abuse of a dominant position post-merger[44]. EU competition enforcement has in the past been deployed for more specific policy ends, such as to deregulate the telecommunications market[45]. Specifically, Article 21(4) of the Merger Regulation provides for Member States to apply additional controls in order to protect media plurality, which responds to concerns that concentration in the media industry could undermine editorial independence and freedom of expression provided for under Article 11 of the Charter[46].

'Even if they serve different goals,' according to a joint report on Competition Law and Data published in May 2016 from the French and German competition authorities, 'privacy issues cannot be excluded from consideration under competition law simply by virtue of their nature'[47]. Data protection authorities can help shed light on how and to what extent the control of personal data is so crucial for companies in markets. The synergies between the fields of law, which have been discussed intensively in the recent years, could propel closer cooperation between authorities, especially where there is neither guidance nor case law. It is not a question of 'instrumentalising' another area of law but rather of synchronising EU policies and enforcement activities, adding value where a supervisory authority lacks expertise or legal competence in analysing.

3. Opportunities for working together

The Digital Single Market Strategy contains many promising suggestions for improving the consumer and data protection regulatory frameworks. However, the strategy could be improved by a mechanism for coherent enforcement across the different fields of EU law of obligations relating to the rights and interests of individuals[48]. From a fundamental rights perspective, the strategy ought also to have addressed how most people interact with the Internet today, with everyday web-based services relying on increasingly granular surveillance of users by service providers, which stands often in contrast to the opacity of how those same service providers process personal information (known as the 'black box' phenomenon).

The recent Commission Communication on online platforms recognised that cross-border nature of the business called for 'good cooperation between relevant authorities'[49]. The 2016 resolution of the national Data Protection Authorities in Europe went further in urging 'a greater dialogue and information sharing with other regulatory bodies responsible for safeguarding the rights and interests of the individual in the digital society and economy', by acknowledging the efforts to strengthen the synergies between regulatory frameworks for consumers, antitrust and data protection[50]. As part of good governance principles and the principle of sincere cooperation, data protection authorities should in any case cooperate with EU agencies and national regulatory authorities with competences in other policy areas[51]. A working party from the Commission's Joint Research Centre argued for a specialist agency to provide technical support to supervisory bodies investigating cases in the digital market and monitor the compliance of online platforms to facilitate 'coherence between regulators in their respective domains'[52].

Ways in which joint working could be of value to regulators include:

- considering the longer term consumer impact of digital concentrations - such as Facebook-WhatsApp, and whether the undertakings or statements from parties to the merger, given at the time, have been subsequently fulfilled;

- any cases which involve unfair terms and conditions and data use policies are obvious opportunities for data protection authorities and consumer enforcers to collaborate, and also for competition authorities where the terms are applied by dominant undertakings in a market;

- cases of dominant companies which behave in a way that may harm the interests of consumers or exclude privacy-friendly competitors would equally be obvious opportunities for dialogue between competition and consumer and/or data protection authorities: for example, a start-up has lodged a complaint against the allegedly dominant mobile operating system for excluding from its application store an app which enables users detect and block third-party services that track them or potentially releases malware[53].

We consider that Article 80 General Data Protection Regulation provides a significant opportunity for collective enforcement. Member States need to apply this provision on collective redress without requiring a specific mandate from a data subject. Advocacy groups have already begun to bring actions under both consumer and data protection rules, for example:

- UFC- Que Choisir and the Federation of German Consumer Organizations (VZBV) introduced action against social media and online services providers for unfair contract terms, unfair commercial practices and infringements of data protection legislation[54];

- the Norwegian Consumer Protection Council issued a study on standard terms used by seven cloud service providers, providing comparative overviews of several terms, including privacy policies. The study led to a complaint about Apple's terms with the Norwegian Consumer Ombudsman for violating Norwegian and European Consumer Law. Apple agreed to amend its terms, and in particular its unilateral right to change the agreement at any time, at its own discretion and without giving users any notice[55];

- an Austrian consumer protection organisation has challenged the terms and conditions unilaterally imposed by Amazon on grounds of the Unfair Contract Terms Directive and the Data Protection Directive. (The CJEU in August ruled on the jurisdictional questions referred to it[56].)

Joined-up enforcement and overcoming ‘regulatory fragmentation’ has now become an urgent need, recognised by the European Commission, with President Juncker at the beginning of his mandate called for the Commission to overcome silo mentalities, and by BEUC, the European Consumer Organisation[57]. Now is an ideal moment to turn these theoretical synergies into positive action.

IV. FOSTERING PRIVACY AND PRIVACY-ENHANCING TECHNOLOGIES AS A COMPETITIVE ADVANTAGE

1. Trust and tracking

There is a widely acknowledged problem with trust and perceived lack of control over what happens in the online environment[58]. In 2015, the New America Foundation Ranking Digital Rights project surveyed many of the biggest companies in the tech sector and judged that each failed basic standards of privacy and censorship – failing for example to disclose when they edited or removed someone's content, scoring low for encryption of private content[59]. We have therefore strongly advocated efforts by the EU to remedy this trust deficit, by encouraging accountability and transparent business models, freedom of choice, data portability and user control, and effective redress in case of infringement of rights. Most recently, in response to the recent consultation on the reform of the ePrivacy Directive, we have advised the Commission[60]:

1. that other than for first party analytics, no electronic communications should be subject to tracking – by cookies, device fingerprinting or any other means - without freely given consent which the individual can easily revoke if she chooses;

2. that individuals should have the right to choose what third party content is allowed or blocked;

3. to ban 'cookie walls' which in effect deny access to websites unless the individual consents to generalised tracking which is not necessary for the performance of the service;

4. to require browsers and other software or operating systems to offer by default controls that make it easy to express or withhold consent to tracking.

A dominant player according to competition case law has a 'special responsibility not to allow its conduct to impair genuine undistorted competition in the common market'[61]. In digital markets, such dominants have been accused of excluding by their conduct new entrants offering more privacy-friendly services, such as those which do not track individuals' online activity except where technically necessary for the provision of the service. Private sector initiatives such as the World Wide Web Consortium's Do Not Track standard, intended to address hidden monitoring of users, have yet to succeed. Partly as a result of this, adblocking has emerged as a popular tactic to evade targeted advertising, which in turn has elicited the counter-response of adblocking detection scripts used by publishers trying to prevent or even to ban their use[62].

In fact targeted advertisement is not *in itself* a fundamental rights issue. More relevant to privacy, data protection and other fundamental rights and freedoms is the need for accessible options for individuals to take control of personal information about them. Concentration of personal data in fewer and fewer corporate hands with limited or no possibilities for individuals to retrieve all data concerning them was never the intention of the pioneers of the Internet. Indeed, one project, led by the inventor of the World Wide Web, aims to reverse this trend by developing a system of decentralised social applications with individual consumers in control of 'where, how and with whom' their personal data are shared[63].

2. Privacy as a factor of quality, and determing the true price of 'free' services

Quality of a product or service, one of the parameters of competition, is in multi-sided markets 'multifaceted' and 'indistinct' and so hard to define, but it remains valid in competition analysis[64]. Privacy and standards of data protection and data security are parts of this quality parameter. Where privacy offered by a web-based service is degraded, this represents consumer detriment which is relevant for both competition enforcement and consumer protection[65]. Issues of transparency and fairness in terms and conditions of several online services have been raised through some national investigations into social media and other online services, such as the German investigation into Facebook's possible 'abuse of market power by infringing data protection rules'[66].

Determining the ability of the company to raise the price becomes problematic for 'free' services, as there is currently no common standard for measuring the actual price of such offerings. However, services priced at zero by profit-maximising firms are as much a concern for authorities as services offered at any other price, though until recently investigations were rare. Where information is extracted for some purpose other than improving the quality or decreasing the cost of a zero-priced product, the amount of information extracted, and the adverts which take up their attention are in effect a cost to consumers. Zero prices carry substantial implications for consumer behaviour and demand, and customers make subjective and not necessarily rational judgements about the cost in terms of attention and information and the quality of the product. Enforcement should aim to ensure that where there are zero priced services, customers get the best possible quality and choice at the lowest possible cost in terms of information and attention[67].

3. Imbalances within the digital transaction

If, as noted above, the harvesting of personal data is, in the digital sphere, a proxy for price, then the share of the 'digital dividend' between controller and data subject, trader and consumer, is more uneven than ever. Dominant platforms are able to discriminate by combining knowledge they extract from data with monopoly power and vertical integration in the markets. Unfair and deceptive practices do occur – as revealed by the enforcement 'sweep' in 2012 by European consumer protection authorities[68]. It is questionable whether it can be fair to subject individuals to terms and conditions for online services which would require on average 25 days a year to read them. Competition should benefit consumers on price, quality and choice[69]; but without competition, if consumers have no options, there is no incentive for a monopoly to deliver good service[70].

Transparency about data use is necessary but, if no realistic alternative exists, it simply leads to a take-it-or-leave-it situation for users: a concern relevant to the German Facebook case[71]. Such web-based services are characterised by information asymmetry, where individuals or small companies lack contextual knowledge about the price and quality of a product, while large companies can rely on flows of information to price and risk management profiles in order to maximise their ability to extract surplus from consumers[72]. Data protection and consumer enforcers are uniquely well equipped to advise on these developments.

4. Weak market for privacy-friendly services

The market for Privacy Enhancing Technologies ('PETs') - measures for minimising personal data processing without losing the functionality of a product or service - remains weak[73]. Privacy is a universal human need, in spite of the willingness of many to disclose intimate details via social media, and the lack of competition over privacy implies market failure[74]. There

is now, with the General Data Protection Regulation, a legal requirement for developers to have regard to 'data protection by design' and 'data protection by default'. The new right to data portability contained in the General Data Protection Regulation if properly implemented and enforced should help individuals to avoid being locked into web-based services. We have also argued that the rules currently under review on confidentiality of communications - one element of the right to privacy - need be applied effectively to all digital communications and not only traditional telecommunications[75]. These legislative developments provide minimum standards for protection, but they do not necessarily create the market conditions in which privacy and freedom of expression become an object for competition[76]. Supervisory authorities cooperating more on how they deploy the existing tools is also necessary to encourage more such competition and to tackle anticompetitive behaviour that frustrates innovation or diminishes privacy as part of the quality of a product.

V. RECOMMENDATIONS: SHAPING AN EU CYBERSPACE BASED ON EU VALUES

Under Article 51 of the Charter, 'institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and [...] the Member States only when they are implementing Union law' are required to 'respect the rights, observe the principles and promote the application' of the provisions of the Charter 'in accordance with their respective powers [...]'[77]. The TFEU also requires the EU to 'ensure consistency between its policies and activities'.[78] Policymakers and authorities are seeking ways to spread to the widest possible public the benefits of Big Data connectivity, powerful computing and ubiquitous and instantaneous data flows. The European Parliament has recently called for the EU to overcome legal fragmentation when drafting new legislation and to encourage a high level of coherence when Member States implement EU law[79]. The EU institutions lead by example and should ensure such coherence in the protection of fundamental rights set out in the Charter. This requires using existing EU tools to create the conditions in which these rights and freedoms can flourish and joined-up enforcement to exploit the synergies between the relevant areas of law. We would like to suggest three practical steps to help do this.

1. Better reflect the interests of the individual in big data mergers

EU merger control has until now focused on companies which meet certain turnover thresholds, unless cases are referred by the national authorities. There are now indications of greater scrutiny of proposed acquisitions of less established digital companies, which may have accumulated significant quantities of personal data that have yet to be monetised[80]. We support this and would offer the expertise of independent data authorities in advising on how to assess the significance for consumer welfare in such proposed acquisitions.

Furthermore, the Merger Regulation should be interpreted, and at the next opportunity amended, to protect the rights under the EU Charter to privacy, data protection and freedom of expression online, just as it currently provides for protection of media plurality. Member States should be permitted also to protect these rights as 'legitimate interests compatible with the general principles and other provisions of the Community Law'[81].

2. A digital enforcement clearing house

Our analysis leads us to the conclusion that there is now an urgent need for coherent enforcement of digital rights in all domains of law regulating online markets. The EU applies a number of different regulatory tools in pursuit of similar ends – fairness, market integration and consumer welfare. Competition enforcement has been so effective not only because of the level of the fines but also because it disrupts how companies and organisations behave. The newly reinforced regimes for data protection and consumer protection could thus emulate competition law by requiring changes, for example, to how personal data is handled which improve overall fairness and consumer welfare.

We therefore propose to facilitate a Digital Clearing House[82]. The Clearing House would be a voluntary network of contact points in regulatory authorities at national and EU level who are responsible for regulation of the digital sector, which might also include authorities such as those in the telecommunications area who supervise the implementation of rules on confidentiality of communications. The two criteria for joining this network would be:

1. **a shared aim** of mutually enhancing their respective enforcement activities and of delivering the best outcome for individuals' rights and welfare, whether as consumers or data subjects;

2. **a willingness to share information and to collaborate** within the boundaries of legal competences and respecting the confidentiality of investigatory activities.

The Digital Clearing House could carry out the following activities:

1. discussing (but not allocating) the most appropriate legal regime for pursuing specific cases or complaints related to services online, especially for cross border cases where there is a possible violation of more than one legal framework, and identifying potential coordinated actions or awareness initiatives at European level which could stop or deter harmful practices;

2. using data protection and consumer protection standards to determine 'theories of harm' relevant to merger control cases and to cases of exploitative abuse as understood by competition law under Article 102 TFEU[83], with a view to developing guidance similar to what already exists for abusive exclusionary conduct;

3. discussing regulatory solutions for certain markets where personal data is a key input as an efficient alternative to legislation on digital markets which might stifle innovation;

4. assessing the impact on digital rights and interests of the individual of sanctions and remedies which are proposed to resolve specific cases;

5. generally identifying synergies and fostering cooperation between enforcement bodies and their mutual understanding of the applicable legal frameworks, including through more informal and formal contact between the European Competition Network, the Consumer Protection Cooperation Network and the Article 29 Working Party (in 2018 to be replaced by the European Data Protection Board).

The Digital Clearing House could begin with a few willing authorities who agree to share contact details and share information, subject of course to the limits of their competence, to their independence of action and initiative and to the confidentiality of their enforcement procedures. The EDPS is ready to facilitate and to support setting up and maintaining this network.

3. An EU values-based common area on the web

The state has a positive obligation to secure respect for private life 'even in the sphere of the relations of individuals between themselves'[84]. We believe the EU should move beyond the current tendency for monitoring of online behaviour, and consider the feasibility of a common area for individuals to interact without fear of being tracked and unfair inferences made about them, a notion which has been recommended by various studies in recent years[85]. This could aim to disrupt the binary choice between 'free' services which are only financially viable through tracking for advertising and paid-for services which users now tend to shun: privacy is not a luxury but a universal right and it should not only be available to those with the means to pay. The common area can be distinguished from the 'digital enclosures' which most Internet users tend now to operate in and which have been criticised by several leading scholars[86]. This would need to be a genuine common area with appropriate safeguards and full respect of the EU Charter, including the conditions governing any limitations on rights and freedoms set out in Article 52(1).

Services already currently offered without tracking and profiling, for example by civil society or developer initiatives, could serve as a model and a pool of experience for the promotion of new approaches. At the same time, EU authorities should encourage the practical application of technical solutions to respect the users' expressed preference on protecting their privacy, such as by clarifying how the W3C's Do Not Track standard should be applied as a data protection instrument, and should explore how the extended enforcement powers under the reform of data protection framework could support this objective.

We will facilitate a discussion with the European Commission and other EU institutions, and we invite all stakeholders to deepen this conversation[87].

VI. CONCLUSION

Human rights were conceived as means for individuals to be safeguarded against state interference. Antitrust has its roots in political decisions to disrupt abusive monopoly power for the benefit of society at large. Consumer rights emerged as a bulwark against abusive traders.

Big Data opportunities for boosting productivity and connectivity should be accompanied by Big Data Protection safeguards. The EU in recent years has shown great leadership in seeking to stimulate a race-to-the-top on privacy standards in the digital arena. The General Data Protection Regulation provides a benchmark for protecting personal data in the digital economy. For a digital economy and society founded on the EU's values, the EU can still do more with the tools available to ensure privacy friendly, fundamental-rights-enhancing products and services. Enhanced transparency, fair treatment, effective choice, absence of market foreclosure for non-tracking models are all entirely compatible and complementary goals.

The Digital Single Market Strategy is the right opportunity for the EU to work coherently towards these goals. Effective enforcement of EU law existing rules is of paramount importance. We believe our recommendations for a Digital Enforcement Clearing House, together with a more holistic approach to concentration and the promotion of an EU values-based common area, would be important steps forward. At a time when data protection and privacy laws are proliferating around the world, this should be a platform for greater bridge-building to other regions of the world, permitting greater dialogue and cooperation with all countries facing the same digital challenge.

This is not the final word on this discussion. The EDPS intends to continue to facilitate discussions and help to break down silos which hinder the protection of the interests and rights of the individual.

Brussels, 23 September 2016

Giovanni BUTTARELLI
European Data Protection Supervisor

Notes

[1] EDPS Preliminary Opinion '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.
[2] 'Report of workshop on Privacy, Consumers, Competition and Big Data 2 June 2014'; https://secure.edps.europa.eu?EDPSWEB/webdav/site/mySite/shared/Documents/consultation/Big%20data
[3] COM (2015) 192 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, A Digital Single Market Strategy for Europe.
[4] EDPS Opinion 7/2015, Meeting the challenges of Big Data.
[5] Certain technical issues relating to competition analysis from the Preliminary Opinion, such as the definition of markets and the role of data as an essential facility, are not further developed specifically in this Opinion which focuses on the major areas for coherent application of data protection, consumer and competition rules. These aspects may be the subject of more structured discussions between regulators which we intend to facilitate.
[6] EDPS Opinion 4/2015, Towards a new digital ethics.
[7] Report of the Special Rapporteur on the promotion and protection of the right of opinion and expression, David Kaye, 22 May 2015.
[8] Ocello, E., Sjodin, C. & Subocs, A. (2015): 'What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case', European Commission--Competition merger brief, 1, 1-7.
[9] Tim Berners Lee argued that the Web owns the potential of being a great equalizer, 'only if we hardwire the rights to privacy, freedom of expression (...) into the game'; . http://webfoundation.org/2014/12/recognise-the-internet-as-a-human-right-says-sir-tim-berners-lee-as-he-launches-annual-web-index/ [accessed 17.09.2016]. See also, for example: Nissenbaum H. and Howe, D., 'Track me not: resisting surveillance in the web search'; Julia Angwin *Dragnet Nation: A Quest for Privacy, Security and Freedom in a World of Relentless Surveillance*, 2014.
[10] 'Competition Law and Data', Autorité de la Concurrence and Bundestartellamt, May 2016.
[11] On the prospect of pricing algorithms eventually leading to Artificial Intelligence colluding in an anticompetitive and probably unethical way, see Ezrachi, Ariel and Stucke, Maurice E., Artificial Intelligence & Collusion: When Computers Inhibit Competition, 2015 (April 8, 2015). Oxford Legal Studies Research Paper No. 18/2015; University of Tennessee Legal Studies Research Paper No. 267.
[12] See EDPS, Meeting the challenges of Big Data.
[13] Financial Times Global 500.
[14] Monopolkomission report, 'Competition policy: The challenge of digital markets', 2015, p. 36.
[15] Article 3(1) of the Commission's proposed directive states that the directive shall apply to contracts under which 'a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data'. Article 3(4) excludes from its scope contracts in which consumers provide only the bare minimum of personal data 'strictly necessary for the performance of the contract or for meeting legal requirements and the supplier does not further process them in any way incompatible for this purpose'. The Commission's proposal accepts the principle that personal data can play the role of money, although it questionably excludes from the scope situations where the supplier collects personal data 'without the consumer actively supplying it': COM (2015) 634 Final, Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts on the supply of the digital content.
[16] Costa-Cabral, F. and Lynskey, O., 'The Internal and External Constraints of Data Protection on Competition Law in the EU', LSE Law, Society and Economy Working Papers 25/2015, p. 11.
[17] Brown I., Marsden C., Regulating Code: Towards Prosumer Law? February 25, 2013 available at: http://dx.doi.org/10.2139/ssrn.2224263 [accessed 17.09.2016].
[18] 'In 1990 the top three carmakers in Detroit between them had nominal revenues of $250 billion, a market capitalisation of $36 billion and 1.2m employees. In 2014 the top three companies in Silicon Valley had revenues of $247 billion and a market capitalisation of over $1 trillion but just 137,000 employees'; 'The Rise of the Superstars, The Economist, 17.09.2016.
[19] 'Competition and privacy in markets of data', speech by Joaquín Almunia, Brussels, November 2012, arguing that 'DG Competition has yet to handle with a case in which personal data were used to breach EU Competition Law'; http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm [accessed 17.09.2016].
[20] Several studies argued that behavioral markets are prone to market failures, which decrease social welfare, and a market failure does occur regarding online privacy, where the behavioral advertising business model 'seems almost designed to take advantage of the bounded rationality'. See Borgesius, F. Z., 'Behavioural Sciences and the Regulation of Privacy in the Internet, Nudging and the Law - What can EU Law learn from Behavioural Sciences'; Acquisti, A., 'The Economics of privacy and the economics of personal data', The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, 2010, http://www.oecd.org/sti/ieconomy/46968784.pdf [accessed 17.09.2016].

[21] 'Refining the EU merger control system', Speech by Commissioner Vestager, Studienvereinigung Kartellrecht, Brussels, 10 March 2016.
[22] On the rights-based European approach to privacy and data protection with close relations to human dignity and self-determination, see for example, Consumer Privacy in Network Industries, A CERRE Policy Report, 26 January 2016, pp. 35-36.
[23] *Z v Finland*, no 22009/93, ECHR 1997-I, paragraph 95.
[24] Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data , and repealing Directive 95/46/EC (General Data Protection Regulation). The requirement for any personal data processing not to be excessive in relation to the purposes for which they are collected and/or further processed was already provided by Directive 95/46/EC, Recital 28 and Art. 6(b) in relation to the data quality principle.
[25] Article 5.1(c) and Articles 14 and 15.
[26] As of June 2014, the Directive EC/2011/83 on Consumers' Rights has repealed the distance Selling Directive 97/7 and the Doorstop Selling Directive 85/577. The EU Consumer Law acquis has been currently undergoing a whole review process and REFIT test.
The new Regulation (EU) 2016/679 on protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC , whose proposal was made by the Commission in January 2012, has been finally published on 4 May 2016.
[27] Judgment of 3 May 2014 in case C-131/12 *Google Spain SL and Google Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzalez.* In this case, the CJEU clarified that the operator of a search engine which orients its activity towards the inhabitants of a Member State of the EU was subject to EU data protection law.
[28] Report of the EDPS workshop on Privacy, Consumers, Competition and Big Data, Bruxelles, 2 June 2014; Workshop 'Trading in Big Data: if data is the new oil, how should its extraction be regulated?' Brunel University, London, 20 April-1 May 2015; Sir Charles Bean's 'Independent Review of UK Economic Statistics', March 2016 suggests measuring the consumption of digital products delivered at zero price by means of the value of time spent on the Internet and the increase in Internet traffic.
[29] 'Were America's firms to cut prices so that their profits were at historically normal levels, consumers bills might be 2% lower' The Economist, 'The Problem with profits', 26 March 2016.
[30] See Stucke, M.E., and Grunes, A.P., *Big Data and Competition Policy*, OUP 2016, pp. 223-24; The Economist, 'Too much of a good thing', 26.3.2016.
[31] '...a few gatekeeper firms are in the position to control the tracking and the linking of (...) behaviours across platforms, online services and sites for billions of users'; Acquisti A., Taylor C., Wagman L., The Economics of Privacy, 8 March 2016, Sloan Foundation Economics Research Paper No. 2580411, p. 3.
[32] Pew Resarch Centre News Use Across Social Media Platforms, 2016; see also, for example, Pariser, E., *The Filter Bubble: What the Internet is Hiding from You*, 2011.
[33] 'Facebook: Political bias claim 'untrue'', BBC, 10.5.2016; 'Google bans payday lender advertising, *FT*, 11.5.2016.
[34] The ePrivacy Directive provisions generally apply where interference with the confidentiality of a communication is technically necessary for the provision of a service (for instance Articles 2(g), 5(1), 6(5), 9(1), 9(3)). On the use of consent in the General Data Protection Regulation, see note 27 of EDPS Preliminary Opinion 5/2016 on the review of the ePrivacy Directive (2002/58/EC).
[35] Under Protocol 27 to the Treaty on European Union, 'the internal market as set out in Article 3 of the Treaty on European Union includes a system ensuring that competition is not distorted… to this end, the Union shall, if necessary, take action under the provisions of the Treaties, including under Article 352 of the TFEU. Joined Cases C-501/06 P, C-513/06 P, C-515/06 P and C-519/06 *P, GlaxoSmithKline Services Unlimited v Commission*, EU:C:2009:610, paragraph 61.
[36] Fairness in consumer law according to CJEU case law is assessed against the 'average consumer' benchmark (Case C-210/96 Gut Springenheide and Tusky [1998] ECR I-4657, para 31); the principle of fairness in personal data processing is enshrined in Article (8(2) of the EU Charter; Articles 101 and 102 TFEU governing anti-competitive behaviour and abuse of dominance each refer to fairness.
[37] 'To the extent that competition law must consider markets in which personal data is present, competition scholars argue that personal data should be analysed according to its economic characteristics, like any other good or service. In this regard data protection regulation could merely set the 'legal context' in which competitive relationships unfold, and would be no different from other market regulation. For their part, data protection authorities have focused on developing the guiding principles of their nascent field of law, and have dedicated little attention to its interaction with the areas of EU law that preceded it;' Costa-Cabral and Lynskey, 'The Internal and External Constraints of Data Protection on Competition Law in the EU', p. 3. Concerning challenges for achieving redress for individuals harmed by violations of data protection rules, see Fundamental Rights Agency Report On the Access to data protection remedies in EU Member States, January 2014.
[38] Competition law's main goals are the subject of ongoing dispute. On consumer welfare as the main goal see C-209/10 *Post Danmark* and C-67/13 *Cartes Bancaires*, on competitive process and structure (insofar as it is as a good enough indication of impact on consumer welfare) see C-501/06 P *Glaxo*, C-95/04 *British Airways* and C/72.

[39] For example, the Belgian Privacy Commission commissioned a report by ICRI into Facebook's terms and conditions which alleged that the social network's statement of rights and responsibility violated European consumer protection law; http://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf [accessed 17.09.2016].

[40] 14-MC-02 Mesure conservatoire du 9 septembre 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité ; the Information Commissioner's response to the Competition and Market Authority's "Energy market investigation: notice of possible remedies" paper, August 2015; Auditoraat Beslissing n° BMA-2015-P/K-28-AUD van 22 september 2015 Zaken MEDE-P/K-13/0012 en CONC-P/K-13/0013 Stanleybet Belgium NV/Stanley International Betting Ltd en Sagevas S.A./World Football Association S.P.R.L./Samenwerkende Nevenmaatschappij Belgische PMU S.C.R.L. t. Nationale Loterij NV; press release about the German investigation into Facebook is available at http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html?nn=3591568 [accessed 17.09.2016].

[41]Judgment of CJEU 23.11.2006 in C-238/05, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios Bancarios (Ausbanc)*.

[42] In the US, the FTC sent the two merging entities a letter on the urge to continue to honour the promise WhatsApp made to its customers regarding its privacy protection regime, though higher than the one experienced by Facebook users. In the letter, the failure to keep these promises would result in violating the FTC Act, Section 5, prohibiting unfair or deceptive practices. The Commission in its decision on the proposed merger stated, 'Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules;' Commission Decision of 03/10/2014 declaring a concentration to be compatible with the common market (Case No COMP/M.7217 - FACEBOOK / WHATSAPP) according to Council Regulation (EC) No 139/2004. See Competition Merger Brief No. 1/2015, 'Lessons from the Facebook/WhatsApp EU merger case', p. 7.

[43] 'Facebook Grilled by EU's Vestager Over WhatsApp Merger U-Turn', 9.9.2016, http://www.bloomberg.com/news/articles/2016-09-09/facebook-grilled-by-eu-s-vestager-over-whatsapp-merger-u-turn [accessed 17.09.2016].

[44] C-12/03 *Commission v Tetra Laval BV* [2005] ECR I-987.

[45] For a review of case law of where CJEU has considered public policy objectives as possible justifications for breaches of competition rules, and of the protection of fundamental rights as a justification in internal market jurisprudence, see for example Costa-Cabral and Lynskey, pp.29-31.

[46] Notwithstanding paragraphs 1 and 2, Member States may take appropriate measures to protect legitimate interests other than those taken into consideration by the Merger Regulation and compatible with the general principles and other provisions of Community law.' The three specific categories of interests, which are explicitly identified as legitimate are 'public security' (1), 'plurality of media' (2) and 'prudential rules' (4). (Regulation 139/2004 Article 21(4).) http://ec.europa.eu/competition/publications/cpn/2005_1_19.pdfhttp://ec.europa.eu/information_society/media_taskforce/doc/pluralism/media_pluralism_swp_en.pdf [accessed 17.09.2016].

[47] 'Antitrust, Privacy and Big Data', Concurrences, 3 February 2015, Joint EDPS-ERA Workshop, 'Competition Rebooted: enforcement and personal data in Digital Markets', 24 September 2015, Brussels; Round Table at *Autorité de la Concurrence* 8 March 2016, Paris.

[48] See BEUC Strategy, A Consumer-Driven Digital Single Market, September 2015: 'Consumers[in the online environment] often find it hard to navigate, to understand their options and their rights, and to find solutions when things go wrong'.

[49] COM (2016)288, Communication from the Commission, 'Online Platforms and the Digital Single Market, Opportunities and Challenges for Europe'.

[50] Resolution of The Spring Conference of data protection authorities, May 2016, available at: http://www.naih.hu/budapest-springconf/files/Resolution---new-frameworks.pdf [accesed 17.09.2016]. See also EDPS response to the Commission Public Consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy, 15 December 2015; House of Lords, Select Committee of the European Union, 10th Report of Session 2015-16, Online Platforms and the Digital Single Market, 20 April 2016.

[51] Hijmans H., The European Union as a constitutional guardian of Internet privacy and data protection, pp.63-65, http://hdl.handle.net/11245/1.511969 [accessed 17.09.2016]. (A modified version of this thesis was to be published in Summer 2016 by Springer International Publishing *The European Union as Guardian of Internet Privacy*).

[52] JRC Technical Reports, Institute For Prospective Technological Studies Digital Economy Working Paper 2016/05, An Economic Policy Perspective On Online Platform, pp.42-43; https://ec.europa.eu/jrc/sites/jrcsh/files/JRC101501.pdf [accessed 17.09.2016].

[53] EU antitrust complaint filed by Disconnect against Google, June 2015 which the complainant published in full at https://www.document.cloud.org/documents/2109044-disconnnect-google-antitrust-complaints.html [accessed 17.09.2016].

[54] Consumer Justice Enforcement Forum (CoJEF) Enforcement of Consumer rights: strategies and recommendations, May 2016.
[55] The full report of the study is available at: http://fbrno.climg.no/wp-content/uploads/2014/02/2014-05-14-Unfair-cloud-storage-terms_report.pdf [accessed 17.09.2016].
[56] C-191/15, *Verein für Konsumenteninformation v Amazon EU Sàrl*, judgment of 28 July 2016.
[57] President Juncker's Political Guidelines, 15.7.2014, https://ec.europa.eu/priorities/publications/president-junckers-political-guidelines_en [accesed 16.09.2016]; BEUC response to consulation 'Empowering the National Comeptition Authorities to be more effective enforcers', 2016.
[58] Special Eurobarometer 431, data protection, June 2015. See also more recent survey by Opinium Research of 7000 European and Middle Eastern individuals reporting 75% consumers have no confidence in social media brands and marketing companies' data protection. https://f5.com/about-us/news/press-releases/european-and-middle-eastern-consumers-deeply-conflicted-over-privacy-and-security-priorities-19968 [accessed 17.09.2016]; The European Commission stated that 'the future of Internet cannot succeed without trust of users in online platforms and without online platforms respecting all applicable legislation and the legitimate interests of consumers and other users. Commission Staff Working Document 'Online Platforms, Accompanying the Document" Communication on Online Platforms and the Digital Single Market"', p. 44. See also speech by Commissioner Vestager, 'Making data work for us', Data Ethics event on Data as Power, Copenhagen, 9 September 2016 : 'Consumers use search engines... [and]... social networks ... And they don't pay a single penny for those services. Instead, they pay with their data. That doesn't have to be a problem, as long as people are happy that the data they share is a fair price to pay for the services they get in return. Personal data has become a valuable commodity. But it can only be sustainable if people trust the companies that collect their data when it comes to the way that they use it. And that trust is not yet there.'
[59] 'No company in the Index provides users with sufficiently clear, comprehensive, and accessible information about the practices they have in place that affect freedom of expression and privacy. These include the handling of user information, terms of service enforcement, government requests and private requests'; https://rankingdigitalrights.org/index2015/findings/ [accessed 17.09.2016].
[60] Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), 22 July 2016, pp.14-16.
[61] Case 322/81, Michelin v Commission, para 70; see page 18 of EDPS Preliminary Opinion
[62] Much of the debate on adblocking detection technologies also focused on whether detecting ad delivery entails storage of personal information under Article 5(3) of the ePrivacy Directive and on the subsequent need to obtain user's consent for running adblocking detection.
[63] The project is called 'Solid (derived from "social linked data")', described as 'a proposed set of conventions and tools for building decentralized Web applications based on Linked Data principles. Solid is modular and extensible. It relies as much as possible on existing W3C standards and protocols'; https://github.com/solid/solid [accessed 17.09.2016].
[64] OECD, The Role and Measurement of Quality in Competition Analysis, 2013.
[65] House of Lords Report, p.102. See Ezrachi and Stucke, The Curious Case of Competition and Quality, Journal of Antitrust Enforcement 2015,1.
[66] Consumer Justice Enforcement Forum (CoJEF) Enforcement of Consumer rights: strategies and recommendations, May 2016.
[67] See, for example, Evans, D. S., Antitrust Economics of Free (April 17, 2011), Competition Policy International, Spring 2011); and Newman, J. M., Antitrust in Zero-Price Markets: Foundations (July 31, 2014), University of Pennsylvania Law Review, Vol. 164; University of Memphis Legal Studies Research Paper No. 151): 'Where market analyses are not conducted, there is potential for massive harm to consumer welfare due to systematic underenforcement of antitrust laws.'
[68] Twenty-five authorities checked 330 websites selling digital content and hound that half contained unfair contract terms or unclear information on right or withdrawal or insufficient information on traders identity and how to contact them: CPC Network SWEEP on Digital Content; www.ec.europa.eu/consumers/strategy.../policy.../consumer_policy_report_2014_en.pdf [accessed 17.09.2016].
[69] Commission Communication :guidance on the Commission's Enforcement Priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings [2009] C45/7, 5.
[70] Google/DoubleClick Decision, para. 39. Vertical Integration and Concentration are highlighted in the Joint FR/DE Report on 'Competition Law and Data', 10th May 2016 pp. 16-19. Edelman B.G., Does Google Leverage Market Power through Tying and Bundling? Journal of Competition Law and Economics, 11 No. 2, June 2015. On leveraging, see Competition and Markets Authority, The commercial use of consumer data: Report on the CMA's call for information', May 2015, paragraphs 3.60-61.
[71] See footnote 40 above.
[72] See Cohen J.E., *Irrational Privacy?*, 2012; Akerlof, G. The Market for Lemons, Qualitative Uncertainty and the Market Mechanism, Quarterly Journal of Economics 84(3), pp.488-500, 1970; Ryan Calo, R., Privacy and Markets: A Love Story, University of Washington School of Law, Legal Studies Research Paper N. 2015-26 p.27. David A. Friedman has argued that there is a 'deceptive framing' of zero priced products which misleads customers' decision-making process; Free Offers: A New Look, 38 N.M. L. REV. 49, 68–69 (2008) .

[73] Commission Communication COM(2007) 228 final on Promoting Data Protection by Privacy Enhancing Technologies; on the market for PETs see for example 'Hiding from big data', The Economist, 7.6.2014.
[74] CMA, The commercial use of consumer data, paragraph 3.21; Executive Office of the President, President's Council of Advisors on Science and Technology, Report to the President, Big data and Privacy: a technological perspective, May 2014.
[75] Preliminary EDPS Opinion on the review of the ePrivacy Directive.
[76] See EDPS Opinions Towards a new digital ethics and Big Data. See also CERRE report ' Consumer Privacy in Network Industries, Improving Network industries regulation', January 2016 'there are circumstances in which data protection can provide a relevant normative benchmark for competition law' Costa-Cabral & Lynskeyp.15; J.A.T. Fairfield, C. Engel, Privacy as a Public Good, Duke Law Journal, Vol. 65, Dec. 2015, No.3.
[77] Case C-176/12 *Association de mediation sociale v Union locale des syndicats CGT and ors ECLI:EU: C:2014:2, 42*.It has also been argued that the obligations in the Charter apply not only to the public sector but also to 'horizontal' situations between natural and legal persons - 'A fundamental right would be ineffective if it protected only against governments'; Hijmans, pp.43-46.
[78] TFEU Article 7. The Court of Justice of the EU applied a balancing methodology between protection of the structure of the market and the public policy objective of the administration of justice in Wouters; C-309/99 *JCJ Wouters v Algemene Raad*, 2002.
[79] European Parliament Resolution of 19 January 2016 'towards a Digital Single Market Act', paragraph 12.
[80] EDPS Preliminary Opinion 2014, p.30; House of Lords Digital p.47. Monopolkommission Special Report No 68, Competition policy: The challenge of digital markets, pp.110-111.
[81] Council Regulation (EC) N. 139/ 2004 on the control of concentrations between undertakings, Articles 21(4).
[82] The notion of the clearing house is understood as a central agency or informal channel for settling accounts or distributing information or assistance with the aim of increasing efficiency and stability. It is commonly associated with buying and selling financial instruments but there are multiple examples of clearing houses in diverse sectors such as railways, education and even data protection and access to information.
[83] Costa-Cabral and Lynskey argue that there may be a precedent for using another field of law to find a restriction by object in CJEU Case C-32/11 *Allianz Hungária Biztosító Zrt, v Gazdasági Versenyhivatal*, judgment of 14 March 2013.
[84]*Von Hannover v Germany* 2004, Application No 59320/0; *K.U. v. Finland*, no. 2872/02, paragraphs 43 and 48, ECHR 2008.
[85] 'Closer dialogue between regulators from different sectors could lead to a response to growing calls for global partnerships which can create a 'commons' of open data where data and ideas, such as statistics and maps, can flow and be available and exchanged in the public interest, with less risk of surveillance, to give individuals more influence over decisions which affect them'; EDPS Opinion, Towards a new digital ethics, p.10 and footnote 36 which cites several sources promoting similar ideas in this area, Schneier, B., *Data and Goliath, the hidden battles to collect your data and to control your world*, 2015.
[86] See for example, Andrejevic, M., Surveillance in the digital enclosure, The Communication Review 10: 295-317; Zittrain, J., *The future of the Internet and how to stop it*, 2008.
[87] See for example idea proposed during a privacy seminar arranged by the Norwegian Data Protection Authority and a council member of the Norwegian Board of Technology in 2015 on securing domain names which are legally bound to abide by the strict privacy and security rules governing their use; reported in http://www.zdnet.com/article/how-two-remote-arctic-territories-became-the-front-line-in-the-battle-for-Internet-privacy/ [accessed 17.09.2016].