The Rise of Big Data and the Loss of Privacy

Anca D Chirita

Abstract: This chapter offers a classification of personal data based on the study of privacy policies of Google, Microsoft Windows, Facebook, Instagram, Linked-In, and Whisper. It argues that online price discrimination contributes to higher corporate profits and economic inequality. Competition policy intervention is therefore needed to curb this inequality that generates a false impression that a few digital giants are competing on the merit of their 'highly innovative' data-driven products and performance. The chapter argues that knowing a consumer's usage, frequency, preferences, and choices disempowers online consumers.

Keywords: Digital markets, competition law, big data, privacy

1. Introduction

This chapter explains why 'big' data matters and why privacy is now lost as a social norm. In its Opinion, the European Data Protection Supervisor suggested a consumer protection approach to data owned by monopolists.[1] It relied on the essential facility doctrine of intervention where a smaller entrant is foreclosed because it cannot access the data owned by the monopolist. The German competition authority indicated that access to data is a factor indicative of market power.[2]

Both the Opinion and the doctrine of essential facilities[3] are now of little help to competition authorities. Instead, this chapter will evaluate the legal framework to clarify the scope of application of the data protection rules and elucidate whether competition intervention has any merit in its own right. Articles 7 and 8 of the EU Charter of Fundamental Rights and the former Directive 95/46/EC will be mentioned before the chapter fully engages with the recent developments in the area of data protection. In particular, drawing on the risks associated with data processing in both Directive

Anca D Chirita, Lecturer in Competition Law (Dr. iur.), Durham University, UK. Earlier drafts of this article benefited from insightful suggestions and comments from the attendees of the 15th Conference of the International Association of Consumer Law organised by the Amsterdam Centre for the Study of European Contract Law on a presentation entitled 'Consumer Rights, Misleading Advertising and Privacy in the Digital Age' in June 2015; LLM students taking a research-led competition law seminar at Durham University in March 2016; the Durham Law School Staff Seminar Series 2015/2016 in May 2016, with special thanks to Aoife O'Donoghue, Se-Shauna Wheatle, Annika Jones, Johanna Jacques, Andrés Delgado Casteleiro, Henry Jones and Professors Thom Brooks and John Linarelli; and the attendees of the conference on 'Personal Data in Competition, Consumer Protection and IP Law: Towards a Holistic Approach' at the Max Planck Institute for Innovation and Competition in Munich in October 2016. The chapter is dedicated to my sister, Andra Chirita, an IT developer, in loving memory.

AD Chirita
Durham University, UK
E-Mail: a.d.chirita@durham.ac.uk

[1] See European Data Protection Supervisor (2014).

[2] Bundeskartellamt (2016) 16; for the view that data can be a source of market power, see Max Planck Institute for Innovation and Competition (2016).

[3] For the view that the doctrine is potentially misleading as rivals are not prevented from collecting data themselves, see Schepp and Wambach (2016) 123.

EU/2016/680 and Regulation EU/2016/679, the chapter seeks to determine how price discrimination can actually happen in the form of abuse of personal data. The latter carries an economic significance, as through the misuse of such data, consumers can be left worse off when bargaining or shopping online. Further risks associated with the processing of personal data concern health, which could, in turn, raise life insurance premium rates. In other cases, personal data can reveal a particular economic situation, personal preferences or interests, reliability, or behaviour, which could make price discrimination much easier.

The new regulation mentions the risks associated with online activity and the need to overcome different rules on the protection of personal data, which could distort competition. The major provision is one which explains that the regulation does not apply to a 'purely personal or household activity', including social networking and online activity. This is to be interpreted in the sense that data protection and supervision do not have as a purpose safeguarding the online privacy of individuals. This is significant since many influential commentators have long held that competition law should not become a regulatory tool for intervention in the area of personal data protection.[4] Nonetheless, the regulatory approach to data processing aims primarily to protect employees from businesses that process personal data and that could lawfully disclose such data to the competent authorities in the wake of various investigations. However, the present framework can easily be abused or misused. It is broad on potential data subjects, as it includes 'persons possessing relevant information or contacts'. So anyone's personal data could be saved for unknown purposes.

The chapter moves on to critically review the position of mere silence or inaction in the case of default settings of social networks or web browsers to review the position of informed consent under the new regulation. The chapter argues that recent theories of informed consent place particular emphasis upon the degree of sophistication and the length of privacy policies, rather than affirmative box ticking. There are hidden 'small prints' or pitfalls, such as 'improving customer experience', which make it possible to process personal data without a just cause.

The chapter examines Windows 10, Google, Facebook, Linked-In, Instagram, Snapchat, and Whisper's privacy policies to establish compliance with data protection and reveal which distinctive categories of personal data are being processed. Existing evidence of price discrimination will be used to extract the pitfalls associated with social platforms based on trust and the potential abuse of consumer confidence that such data is safe from being shared with third parties. Although there are warnings regarding the selling of data, this chapter will remain focused on the big data owned by the three main companies, namely, Google, Facebook, and Microsoft. The selling of personal data could potentially lead competition authorities to uncover the bid-rigging of markets for personal data, which could extend competition intervention to include more 'secretive' social media, such as Whisper, Snapchat, or Instagram. Installed software and browsers can also be used as a means to improve users' experience, but the processing of sensitive and confidential data has little to do with this purpose.

This author agrees with the merits of the dissenting opinions by the late Commissioner Rosch and Commissioner Jones Harbour, albeit this author argues that the EU Commission's intervention is warranted by the enactment of the new rules on data protection, in particular, by what these rules have now left outside their material scope. Relying on Stiglitz's theory of economic inequality, this

[4] Recently, it has rightfully been argued that less intervention is inappropriate, see Kadar (2015).

chapter argues in favour of considering data as the new currency in two-sided markets. While Google's sale of its users' privacy to third parties has famously been described as 'Googlestroika', namely, a 'privacy derivative', this zero-priced product[5] remains problematic through the sharing of personal data with third parties.

In conclusion, the chapter adds the abuse of personal data to the non-exhaustive list of abuse of dominance.[6] The latter happens on online platforms, which are outside the scope of data protection laws. Such platforms misuse the trust and confidence of individual users by making them reveal personal data and by encouraging users to voluntarily consent to the transfer of personal data to third parties. Personal preferences or choices are later shared with advertisers and sellers and used to engage in price discrimination. Ultimately, data protection laws are useless in practice,[7] as they solely highlight the need to educate consumers and raise awareness. There is, therefore, one active remedy left: the intervention of competition policy. Indeed, online price discrimination and booking manipulation based on users' personal data is now a social norm.

2. Why Big Data Matters

All businesses, including public institutions, may possess and/or process some form of personal data. This chapter is not concerned about the mere possession of personal data by a dominant market player. Rather, it seeks to highlight how personal data, which is economically relevant, could be misused, for instance, through it being shared with third parties, in order to maintain or strengthen a dominant market position. Furthermore, this chapter also wishes to signal an eventual bid-rigging of personal data by colluding undertakings, including popular social media, under Article 101 TFEU.

This chapter acknowledges that a potential misuse of personal data by dominant undertakings has no precedent line of case law. While its novelty could trigger this particular form of abuse to be affixed with an exotic label, as it sits outside the confines of traditional competition practice under Article 102 TFEU, it is never to be under-estimated by dominant undertakings that actively engage in the sharing, transferring, or selling of such data.

The author is grateful to the Commissioner for Competition, Margrethe Vestager, for bringing data concerns to the competition policy's discourse. In her recent speech,[8] Commissioner Vestager said

> a lot of people tell me they're worried about how companies are using their data. I take those worries very seriously. Privacy is a fundamental part of our autonomy as individuals. We must have the right to decide who we share our information with, and for what purpose.

[5] It is interesting to note that, according to a leading economist, 'Free is a number; it is the price of zero', see the Witness Evidence provided by Evans and Ezrachi (2015) 10; see e.g. Schepp and Wambach (2016) who argued in favour of competition intervention based on data protection and privacy as 'elements of non-price competition', 123; see e.g. Martens (2016) who argued that the widespread market failure of privacy informed decisions by consumers could pave the way for regulatory intervention, 38.

[6] Again, proving Hayek's assertion right, namely, that competition is a process of discovery, this time in the area of new information economics; see Hayek (2002) 9-23.

[7] For the view that data protection law is unable to address the concerns of individuals regarding personal data processing by platforms, see London School of Economics (2015).

[8] Vestager (2016); Committee of Economic and Monetary Affairs (2014) 4-056.

This is the first time that privacy considerations have formed part of meaningful competition policy rhetoric. And this rhetoric can also succeed when these considerations are properly identified and given an economic dimension, which this chapter will seek to achieve in the next sections. Nonetheless, in the 1980s, US scholars were preoccupied by privacy. While Posner's concept of privacy[9] appears limited for current purposes, nonetheless, it represents a historical moment for privacy. Initially, Posner looked at potential labour market asymmetries if employers were not able to have personal data about their future employees. Disclosure was, therefore, seen as mandatory for employees with criminal records. This context of employment relations led Posner to consider privacy as being 'harmful to efficiency' where a lack of disclosure could prevent an efficient exchange of labour. Similarly, Hermalin and Katz argued that, due to these information asymmetries caused by non-disclosure, an individual with poor health could opportunistically take advantage of life insurance.[10] However, such cases are very limited.

For Stigler, privacy is a subject of public policy,[11] whose purpose is 'the possession and acquisition of knowledge about people'. In practice, privacy acts as a shield that restricts the collection or use of personal data about an individual or corporation.[12]

A notable academic commentator had previously remarked that

> the loss of individual privacy (…) is often framed more around an individual sense of unease at the surveillance of peoples' lives than how a shift in knowledge about individuals to corporate hands should force us to re-evaluate our economic models and regulatory tools.[13]

This chapter raises no expectation that competition authorities will tackle the complex issues surrounding individuals' surveillance at large.[14] Instead, the chapter aims to elevate the normative value of privacy as an economic right that is not devalued by public competition enforcement as being solely a human right of the public, which has to be addressed elsewhere and through other means, e.g. consumer or data protection law. Beyond any doubt, competition authorities will have to adapt their traditional law and economics analysis in order to be able to deal with a monopolistic abuse of personal data in digital markets for two main reasons.

First, it is uncontroversial to suggest that personal data owned by companies has, indeed, an economic value attached to it. In the words of the EU Commissioner, such data has become the 'new currency.'[15] Previously, the European Data Protection Supervisor recognised that while

> consumers provide richly detailed information about their preferences through their online activities (…) personal information operated as a currency, and sometimes the sole currency, in the exchange for online services.[16]

---

[9] See Posner (1980) 405-409.
[10] See Hermalin and Katz (2006) 211.
[11] See Stigler (1980) 624.
[12] Ibid 625.
[13] Newman (2014) 852.
[14] See Joyce (2015) 3. This chapter leaves outside its scope the implications of the recently enacted UK Investigatory Powers Act, which received Royal Assent on 28 November 2016, available at http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted/data.htm
[15] Vestager (2016). Similarly, when providing his expert witness on online platforms, Professor Ezrachi suggested that 'the engine, the fire at the heart of this market, is definitely data'; see Evans and Ezrachi (2015) 15.
[16] European Data Protection Supervisor (2014), para. 2.2.10.

Therefore, it is uncontroversial to consider the owners of personal data as consumers of online products or services, from search-engines, shopping, to social or professional media. While trading and entertainment follow different purposes, both can intersect each other; this blurs the distinction between private and public spheres. An axiomatic reduction of competition policy's objectives to consumer welfare[17] means that once a company sells a product for free, but the sum of its individual consumers pays nothing more in return than the naive confidence that any personal preferences, economic interests or behaviour will be kept private, this is an exploitative abuse. Through invasive techniques of data sharing, such companies are guilty of misusing personal data for extracting an economic profit. Personal, private data becomes then public data owned by third parties so that dominant undertakings can further consolidate their dominant position. This has absolutely nothing to do with competition on the merit. If a product or service had been promised for free, but the seller charges a bill for it later, then that product or service is called 'personal data':

> if just a few companies control the data you need to satisfy customers and cut costs, that could give them power to drive their rivals out of the market.[18]

Second, it would be controversial to identify an anti-competitive practice where a few undertakings were to control big data but to use it to eliminate their smaller competitors.[19] Moving in this direction, a recent joint report by the French and German competition authorities has rightfully identified that data itself is 'non rivalrous',[20] while examining the existence of a sufficiently large customer base, network effects, and barriers to market entry.[21]

While the orthodoxy of exclusionary abuse dominates past competition practice, it is by no means a universal remedy for abuse in the present setting. As revealed by various commentators, exploitative abuse[22] often remains unchallenged and under-enforced, as it asks competition authorities to put forward evidence of any anti-competitive harm. For competition and data enforcers, this can easily turn into a daunting task of hunting for hidden evidence of data misuse.

The European Data Protection Supervisor came with a similar exclusionary vision in hindsight. It duly acknowledged that 'powerful or dominant undertakings are able to exploit "economies of aggregation" and create barriers to entry through the control of huge personal datasets'.[23] However, as every dominant, or even non-dominant, company should take full responsibility for its datasets, barriers to entry are never the culprit of the real problem. Raising barriers to entry is costly for competitors, but, as digital products or services are offered for free in exchange for personal data, such dominant companies cannot produce them any more cheaply. Therefore, digging into a hole, i.e. the essential facility doctrine, and seeing dominant companies as gatekeepers of big data who exclude smaller rivals, is nothing but a false premise. The actual problem can be solved only by proving that the data in question is the price to be paid and that privacy can be translated into monetary terms. To put it another way, this chapter argues that competition intervention against 'big

[17] For the argument that consumer law is now closer to the goals of EU competition law, see Albors-Llorens (2014) 173; on the potential to incorporate consumer law requirements into competition policy, see Chirita (2010) 418.
[18] ibid.
[19] See Pasquale (2013) 1009; for the contrary opinion, see Lerner (2014) 19.
[20] Lerner (2014) 21, for the same finding see e.g., Martens (2016) 38.
[21] Autorité de la concurrence and Bundeskartellamt (2016), thus the report relies on the old directive.
[22] For the view that some anti-competitive practices may be both exclusionary and exploitative, see Bellamy and Child (2013) 10064; O'Donoghue and Padilla (2006) 194; for an explanation of the two concepts, see Whish and Bailey (2015) 212.
[23] European Data Protection Supervisor (2014), para. 3.1.4.24-25.

data' monopolists should be based on identifiable economic harm to consumers of digital products or services as a result of exploitation of their naïve trust and confidence. It should not be based solely on crude and rivalrous exclusionary abuse through harm inflicted on other competitors who are attempting to possess the same relevant data.

3. Privacy as a Fundamental Economic Right

Many articles have already been written on the provisions of the EU Charter of Fundamental Rights offering individual protection against interference by the state in the private sphere (Article 7) and beyond to protect personal data (Article 8).[24] This fundamental protection creates an expectation that privacy disclosures are an exception rather than the norm. In sharp contrast, Facebook's owner, Zuckerberg, has claimed that 'privacy is disappearing as a social norm'.[25] However, as the recent investigation of the German competition authority demonstrates, not even Facebook is immune from competition intervention.[26] Article 8's exceptional requirements, namely the fairness and lawfulness of the data processing, for a specified purpose and transparency, are to be considered as setting the constitutional dimension of privacy.[27] The former Directive 95/46/EC[28] conferred individual protection of personal data. Article 2 referred to 'any information relating to an identified or identifiable natural person'. Following this line, privacy entails certain subjective attributes, such as the identity, characteristics, or behaviour of an individual. In particular, Article 6 (1) of the Directive laid down some fundamental principles of data protection. These principles aim to ensure trust, predictability, legal certainty, and transparent use of personal data by data controllers. The collection of personal data is rather exceptional, namely, for 'specific, explicit and legitimate purposes'. Any data processing should be compatible with these purposes. The new EU Directive 2016/680 is more helpful in delimiting the above purposes, namely the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties.[29] Recital 26 in conjunction with Article 46 (1) aim to raise awareness of the risks, rules, safeguards, and rights in relation to the processing of personal data. While 'awareness raising' resonates with the right of consumers to information and education, as embedded into Article 169 of TFEU, the economic interests of consumers are simply put into jeopardy by this lax approach. Again, the European Data Protection Supervisor had previously warned that

[24] See Lynskey (2014) 569-597; in the UK, data protection has been seen as a facet of privacy, see Lynskey (2015) 529; Roberts (2015) 544; Lynskey (2014) 1800.
[25] See the Guardian (2010), Privacy No Longer a Social Norm, Says Facebook Founder (10 January).
[26] Bundeskartellamt (2016).
[27] See, for instance, the constitutional controversy raised by the German bill on data retention, which was criticised by the Federal Data Protection Commissioner as a disproportionate violation of Germans' basic civil rights, see Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*, BT-Drucksache 18/5088.
[28] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to personal data and on the movement of such data, [1995] O.J. L 281.
[29] Directive EU/2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, [2016] O.J. L119/89.

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.[30]

The material scope of personal data processing remains guided by the principles of lawfulness, i.e. necessary for the performance of a task carried out in the public interest by a competent authority;[31] adequacy and relevance, i.e. for the purpose for which data is processed;[32] transparency,[33] i.e. the right to know about the various purposes of data processing; and proportionality, i.e. data should not be kept longer than necessary unless processing could be reasonably fulfilled by other means. In the forthcoming section detailing particular case studies, it will be demonstrated how, in practice, big companies collect an excess of personal data.

Under 'data subjects',[34] the directive includes as addressees of data protection suspects, persons convicted of a criminal offence, victims, and other parties, such as witnesses, persons possessing relevant information or contacts, and associates of suspects and convicted criminals. Given that anyone could be within a circle or network of contacts, which could eventually reveal sensitive information, there is a greater potential for the misuse or abuse of data processing.

Turning back to the previously alluded to risks associated with the rights and freedoms resulting from data processing, both the EU Directive 2016/680[35] and Regulation 2016/679[36] include a long list of potential personal damage due to, for example, discrimination, identity theft or fraud, financial loss, loss of confidentiality, unauthorised reversal of pseudonymisation, or other 'significant economic or social disadvantage'. Some of them find a strong link to competition practice, in particular where the data could be processed for engaging in price discrimination. The latter anti-competitive practice[37] could cause financial losses during shopping or bargaining due to the misuse of personal data about an economic or social condition. Again, this demonstrates that, by ignoring privacy considerations that carry an economic significance, competition authorities could miss out on many opportunities to uncover anti-competitive misuse and abuse of data. Of course, discrimination can be based on many other subjective factors, such as racial or ethnic origin, political opinions, religion, sexual orientation[38] and so on, and so these are not necessarily used for economic or price discrimination. In *Digital Rights Ireland*,[39] the ECJ considered that

[30] European Data Protection Supervisor (2014), para. 2.4.14.
[31] See Recital 35 of the new Directive.
[32] ibid Article 4 (1).
[33] ibid Recital 43.
[34] Ibid Recital 31 in conjunction with Article 6.
[35] Ibid Recital 51.
[36] See Recital 75 of the 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 Protection Regulation), [1995] O.J. L119/1.
[37] Generally on price discrimination, see Bergmann, Brooks and Morris (2015) 921; Baker (2003) 646; Armstrong and Vickers (2001) 579; against regulating price discrimination, see Cooper (1977) 982.
[38] For example, Facebook's users could be targeted with specific advertising based on certain characteristics, such as 'interested in women or men' which had been entered in their profile, see Heffetz and Ligett (2014) 81.
[39] Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications* [2014].

To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way.[40]

Other sensitive data, such as genetic, biometric, or health data, could lead to the price discrimination against individuals in their daily life, for example, when applying for life insurance.[41] For those competition authorities that have, in recent years, adjusted their enforcement efforts to consider aspects of behavioural economics,[42] Regulation 2016/679 places 'personal preferences or interests, reliability or behaviour' in the spotlight of evaluating personal aspects of data subjects' lives. The processing of such behavioural data could also lead to price discrimination. The same applies to aspects concerning economic situation, location, or movements. Ultimately, if personal details are known, those who possess them could engage in price wars based on someone's economic, social, physiological, or health, i.e. genetic or mental condition.[43]

So, how are these categories of personal data linked to competition? One of the most significant provisions of Regulation 2016/679 is Recital 2's reference to the accomplishment of an 'economic union', to 'economic and social progress', and to the 'well-being of natural persons'. While economic goals match competition policy's goals, consumer well-being is, indeed, wider than welfare. However, having regard to earlier considerations, online privacy law[44] affects the well-being of individuals but could be translated into economics of privacy. In other words, personal data forms an integral part of the economic calculus. Contributing to closing the gap between privacy and competition is Roberts' recognition of a right to privacy, whose function is 'to prevent others from acquiring *dominating* power'.[45] In essence, this conceptual threshold advanced by public law matches perfectly the one used by the same preventive function of abuse of dominant market power under competition laws.

Another significant provision is Recital 9 of the above regulation, which acknowledges a 'widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity'. This becomes problematic because of existing differences in the level of data protection. It is yet another 'obstacle to the pursuit of economic activities', which could 'distort competition'.

The material scope of the application of Regulation 2016/679 is reinforced by Recital 18, which makes it clear that the regulation does not apply to the 'processing of personal data in the course of a purely personal or household activity'. This may include 'correspondence, the holding of addresses, or social networking and online activity undertaken within the context of such activities'.[46] As long as online searching, browsing, or social media interactions have 'no connection to a professional or commercial

[40] Ibid, para. 33.
[41] See Evans (2009) 50, who considered the possibility that advertisers could infer from an individual's online behaviour whether the user falls under a low or high insurance risk.
[42] For an excellent book on behavioural economics of consumer contracts, see Barr-Gill (2012) 7; on the limits of competition and the necessity of adding behavioural economics to include misperception and bias caused by asymmetric information available to consumers, 16.
[43] See Article 3 (1) of the Regulation on personal data that could be used to identify someone after name, location, or online identifier and other subjective factors.
[44] See 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, known as the Directive on privacy and electronic communications, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, [2009] O.J. L 337/11.
[45] Roberts (2015) 546 (emphasis added).
[46] See Recital 18 of the new Regulation.

activity', Regulation 2016/679 does not apply. This is of great significance for competition authorities. Many commentators have been dismissive of an eventual competition law intervention in this area without offering any compelling reasons for non-intervention. Therefore, by making a clear distinction between the public or professional profile of an employee and the private regime applicable to personal data, the regulation leaves untouched a grey area of big data owned by digital monopolists. The danger of monitoring individual behaviour or internet tracking or of profiling for analysing or predicting an individual's own personal preferences, behaviour, and attitudes, could never have been made clearer than in Recital 24, albeit in a professional context.

To date, there is no economic regulation applicable to digital monopolies that process personal data unrelated to employment or professional activities. Therefore, the above regulation becomes inspirational for competition authorities to discern the subjective factors related to the private sphere, which could later interfere with consumers' economic decisions, e.g., online shopping or bargaining.

Finally, Regulation 2016/679 clarifies the meaning of 'enterprise' and 'group of undertakings',[47] offering the right to an effective judicial remedy against a data supervision authority[48] and the right to compensation from the data controller or processor for damages.[49] Article 83 foresees fines for undertakings of up to 2 per cent or 4 per cent of their worldwide annual turnover of the preceding financial year in cases of infringement related to personal data processing, including lack of consent.

4. Informed Consent

An earlier report by the European Data Protection Supervisor found that mere silence or inaction in the case of default settings of online social networks or web browsers is not valid consent.[50] It is obvious that prior consent is required before any processing of personal data can occur, and that notice should be given 'in clear and understandable language'. Furthermore, whenever personal information is to be processed, individuals should be entitled to know about it.[51] These recommendations have been included in Regulation 2016/679. In the same vein, 'silence, pre-ticked boxes or inactivity' cannot constitute valid consent. In particular, Recital 32 requires that 'clear affirmative' consent be given with a 'freely given, specific, informed and unambiguous indication' that the individual concerned agrees to data processing. Following this line, ticking a box when visiting a website, choosing technical settings, or another statement or conduct that clearly indicates acceptance of the terms and conditions of privacy, is deemed to pass the test of valid consent. Therefore, informed internet and social media users should avoid ticking any boxes in order to avoid agreeing to unwanted privacy terms. This is because the latter are notoriously very lengthy. As has been suggested, on average, each internet user would need around 244 hours a year to read about privacy policies.[52] Similar to hidden terms and conditions of sale, statements about personal data

[47] See Article 4 (18) and (19) respectively.
[48] See Article 78.
[49] See Article 82.
[50] European Data Protection Supervisor (2014), para. 3.1.4.24-25.
[51] ibid.
[52] McDonald and Cranor (2008) 17; for a similar concern expressed about onerous obligations imposed on consumers when reading, often incomprehensible, privacy policies, see Kerber (2016) 7.

processing are concealed in the 'small print'.[53] As the forthcoming case studies will show, most digital giants have construed privacy using rather mysterious terms, such as 'improving customer experience'.

Regulation 2016/679 draws inspiration from the Council Directive 93/13/EEC on unfair terms when it requires the controller of personal data to demonstrate 'pre-formulated' consent in 'an intelligible and easily accessible form, using clear and plain language'. Previous experiences with the interpretation of what constitutes 'intelligible' under this Directive require less sophistication, whenever possible, in privacy terms. However, under Recital 42 of the Regulation, 'informed' consent expects individuals to be aware of the identity of the controller and of the purposes of personal data processing. This legal innovation is no major overhaul. Knowing the identity of the data processor, or the kind of personal data being processed, does not make an individual immediately aware of all the possible legal consequences of placing trust in a social platform, of browsing, or of downloading software.[54] Similar to the 'take-it-or-leave-it' conceptual framework under the law of contract,[55] the Regulation disregards consent whenever an individual has 'no genuine or free choice or is unable to refuse or withdraw consent without detriment'.[56] Popular digital monopolies, such as Google, Facebook, or Microsoft, offer no free choice compared to alternative services, which could be of inferior quality, be it because they are as yet under-developed or less innovative or be it that they are so because such services do not process significant data from their users. Irrespective of what exactly causes a dominant position to happen, there will always be a significant imbalance between a digital monopolist and its users. As Recital 43 of the Regulation rightfully points out, there will be no valid consent 'where there is a clear imbalance', in particular, where personal data had been processed by a public authority. It is then unlikely that consent was freely given. A presumption of lack of 'free' consent will also operate if 'separate' consent cannot be given to different operations of processing. Alternatively, it is possible that consent was required for the performance of a particular service for which data should not be processed at all. Finally, this chapter argues that a modern interpretation of the traditional doctrine of unconscionability of contracts[57] would be welcome in the context of online platforms and could bridge the conceptual divide between the inequality of bargaining power and the exploitation of weaker and vulnerable consumers.

5. The Case for Competition Intervention against Targeted Advertising

As mentioned earlier, competition law can address two main categories of anti-competitive practices. For example, it could potentially tackle the sale of personal data by colluding companies and trigger repercussions under Article 101 TFEU and Chapter I of the UK Competition Act 1998. There is some speculative evidence which suggests that data can be worth up to $5,000 per person per year to advertisers[58] or up to $8 trillion when including other non-tangible assets.[59] The European Data

[53] See the European Data Protection Supervisor (2014), para. 4.3.2.77.
[54] In the same vein, see Nehf (2016).
[55] See Smith (2005) 12; for the view that the frequency of harsh terms in standard forms of contract is the result of 'the concentration of particular kinds of business in relatively few hands', see Beale (2002) 232; Kessler (1943) 629.
[56] Recital 42 of Regulation 2016/679.
[57] See Bigwood (2003) 247; on the superior bargaining power by monopolists, see Smith (2005) 319; on unconscionability as exploitation, see Smith (2005) 300; Morgan (2015) 211; on the consumers' lack of understanding of privacy policies, see Strahilevitz and Kugler (2016) 20; for the view that informed consent is unrealistic, see Martens (2016) 38.
[58] *Market Watch* (2012).

Protection Supervision advanced that personal data shared when using online platforms exceeds, by far, €300 billion. It is true that users place trust in internet platforms, thereby contributing to the sharing of their own personal data for free.[60] There is, therefore, a far greater potential to tackle the sharing of personal data by digital monopolists given the earlier discussion of the forms of acceptable, valid, and informed consent. Both Article 102 (1) (a) TFEU and Chapter II (§18) of the UK Competition Act 1998 refer to the imposition of 'unfair prices' or 'other trading conditions' from which price discrimination could be extracted and unfair terms be inferred.

Earlier attempts to deal with a misuse of data by monopolists failed subject to dissenting opinions. The late US Commissioner Rosch had flagged up that Google's power of monopoly or near-monopoly in the search advertising market could be attributed to its 'power over searches', i.e. user data, through deceptive means.[61] However, Commissioner Rosch was sceptical about imposing on monopolists 'a duty to share data' with their rivals.[62] Indeed, such a duty could even run counter to the new data protection framework in the EU. In the US *Google/DoubleClick* merger, the Federal Trade Commission rejected privacy considerations from its analysis.[63] The FTC lacks competence over privacy, and there is no robust but instead only fragmented data protection subject to various pieces of legislation.[64] In her dissenting opinion, Commissioner Jones Harbour[65] considered the merits of privacy considerations. She rightfully argued that Google/DoubleClick will gain unparalleled access to consumers' data as a result of the merger.[66] The merger has allowed Google to track both users' Internet searches and their web site visits. Similarly, Facebook sought to incorporate the information shared by WhatsApp users into its consumer profiling business model.[67]

The above cases represent missed opportunities to challenge 21st century anti-competitive and strategic practices concerning personal data in digital markets. The Sherman Act became law in 1890, the Federal Trade Commission's Act in 1914 – both antitrust laws are lagging behind the digital revolution. Objectively, Section 5 of the FTC's Act on unfair and deceptive advertising alone could not have sufficed before the US courts given that a data protection framework is missing from the landscape.[68]

Comparatively, the EU Commission has dealt with issues related to data in the *Microsoft/Yahoo!Search* merger case[69] involving the acquisition by Microsoft of Yahoo's internet search and advertising. The Commission considered that a new entrant will have to overcome barriers to entry and, as a result, could incur 'significant costs' associated with developing and updating the

[59] *The Wall Street Journal* (2014).
[60] See also Newman (2014) 850.
[61] Concurring and Dissenting Statement of Commissioner J Thomas Rosch Regarding Google's Search Practices, In the Matter of Google Inc., FTC File No 111-0163, [2012].
[62] ibid 6.
[63] FTC, *Google/DoubleClick*, File no 071-0170, [2007].
[64] See Stigler (1980) 624, who mentioned the Privacy Act of 1974 on the control and access to information about individuals by the federal government; the Fair Credit Reporting Act (1970) or employment laws prohibiting 'the collection or use of sensitive information about sex, race, or physical handicaps'; the Bank Secrecy Act of 1970; the Equal Credit Opportunity Act; Title VII of the Civil Rights Act of 1964; the Genetic Information Nondiscrimination Act etc.
[65] Dissenting Statement of Commissioner Pamela Jones Harbour, In the Matter of *Google/DoubleClick*, FTC File No 071-0170.
[66] ibid 8.
[67] European Commission, Case M7217, *Facebook/WhatsApp* [2014] O.J. C297.
[68] See the efforts of the FTC for ensuring 'Do Not Track' rules for web browsers, data portability, greater transparency, and express consent when collecting sensitive, e.g. health, data, in 'Protecting Consumer Privacy in an Era of Rapid Change' (March 2012).
[69] EU Commission, Case M5727, *Microsoft/Yahoo!Search Business* [2010].

search algorithm. The latter would need to have 'a large database'.[70] Although the decision did not consider privacy, it did raise a relevant issue with regard to the transfer of data by advertisers from one system to another.[71] In the *Google/Double Click* merger case,[72] the Commission emphasised the pro-competitive benefits in the form of network effects. The latter stemmed from serving commercial ads due to the 'large amounts of customer-provided-data' compared to the more limited amounts of data collected by competitors.[73] However, the Commission was not concerned about privacy at this stage; quite the contrary, it went on to mention that the collection of data allows for 'better targeting of ads' by advertisers.[74] Later, the Commission clarified that DoubleClick does not use behavioural data for the purpose of 'improving ad serving' to third party publishers or advertisers.[75] Ultimately, the Commission eventually acknowledged that

> particularly large internet service providers could thus try to team up with advertisement companies to make use of this data under the restrictions imposed by privacy rules, but they could also try to use this data with their customers' consent, for instance in exchange for lower prices.[76]

While the Commission mentioned the legal framework of privacy rules, it did not thoroughly investigate the economics of privacy, in particular, targeted advertising. It simply assumed that customers could have sufficient bargaining power to extract lower prices.

Another missed opportunity – this time in the UK - of dealing with an alleged online discrimination in the search market for online maps is *Streetmap.*[77] It demonstrates how Google's competitors are having a very hard time proving an 'objective' abuse of dominance[78] on the basis of this monopolist's exclusionary conduct alone, and why it would have been helpful to prove anti-competitive harm to consumers in order to strengthen the subjective, i.e. exploitative, side of abuse. Apart from this, the High Court of England and Wales stumbled when it refused to admit that, under Article 102 TFEU, there is no *de minimis* doctrine applicable so as to expect an 'appreciable effect in the market for online maps'.[79]

So is it right to believe that privacy is solely a consumer protection issue and not, as yet, a competition law issue? Consumers are often unaware who has access to their personal data; what kind of data is processed; and how, when, and where it is shared or sold.[80] No individual consumer can stand alone in the fight against big data owners. Competition law is, ultimately, the proper solution to online data misuse or abuse.

Critics have argued convincingly that competition law offers a 'convoluted and indirect approach' to online privacy.[81] They have suggested that a unified enforcement of traditional competition and

---

[70] Ibid, para. 111.
[71] Ibid, para. 140.
[72] European Commission, Case M4731, *Google/DoubleClick* [2008].
[73] Ibid, para. 179.
[74] Ibid, para. 182.
[75] Ibid, para. 182.
[76] Ibid, para. 271.
[77] *Streetmap EU Limited v Google Inc.* [2016] EWHC 253 (Ch) (12 February 2016).
[78] Ibid, para. 56, where the High Court re-hearses well-known verses from Case 85/76, *Hoffmann-LaRoche v Commission*, [1979], para. 91.
[79] Ibid, para. 98; also, see Whish (2016) who clarifies the misunderstanding and subsequently comments on *Streetmap.*
[80] See Grunes and Stucke (2015) 12, who support the view that ignoring privacy as a sole consumer protection issue is wrong.
[81] Ohlhausen and Okuliar (2015) 156.

consumer issues could 'destabilise the modern consensus on antitrust analysis', dismissing 'rigorous, scientific methods' to favour 'subjective noncompetition factors'.[82] In sharp contrast, Edelman concluded one of his seminal works on Google with an emphasis upon 'decades-old competition frameworks', which remain 'ill-suited' for fast-moving digital markets.[83]

It is difficult to grasp how an assessment of market dominance will succeed without rigorous economic assessment and why personal data, preferences, and choices should continue to be misused, thereby putting online consumers at an economic disadvantage vis-à-vis sellers or retailers through third-line price discrimination.[84] If consumers are staring at products on display in shops, nobody records their physical presence to later put up the price.[85] Nor do sellers on the high street know how rich their customers are, where they live, and so on. If online privacy continues to be ignored by competition/antitrust authorities in the digital age, then calls will follow shortly to disempower them and empower instead other competent authorities that will, indeed, stand up for online consumers and deal with the culprits of personal data collection, transfer, sharing, or selling. In this author's view, unlike their US counterparts, the EU competition authorities are sufficiently robust and equally flexible to effectively adjust to the needs of the online economy[86] and to successfully protect European citizens as online consumers.

At a first glance, the concern over privacy could rightfully be seen as the private affair of a naïve and trusting individual. If there were only one such individual, or just a few, out there, then consumer law would suffice. However, the reality shows that this is not the case. Competition law stands out as a branch of public law[87] and, therefore, it cannot turn a blind eye to the sum of privacy losses by online users at large. The data protection loopholes cannot be taken to provide such a speculative, and thus enriching, ground for large businesses.

A contrary, but commonly held, view dismissing competition policy's intervention into data-driven industries relies on the mutual benefits generally brought by dual-sided platforms for both users and owners. In sharp contrast, the European Data Protection Supervisor suggested that

> often companies rely on and exploit big data by operating a two-sided or multisided platform or business model, cross-financing distinct 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.[88]

Empirical research by economists has suggested that it is uncommon for industries based on two-sided platforms to be monopolies or near monopolies.[89] Yet, the contrary is held to be the case when

[82] ibid.
[83] Edelman (2015) 33.
[84] Under the US antitrust law, this type of price discrimination requires proof of harm to the competitive process, rather than an exploitation of consumers, see Hermalin and Katz (2006), 230.
[85] Also, see Acquisti and Varian (2005) 367, suggesting that, while consumers might be aware of online tracking, firms will be using it to 'tailor prices'; Einav and Levin (2014) 12430894, highlighting inter alia that by knowing behavioural data, i.e. individual preferences, sellers could make pricing changes in response to consumer demand.
[86] In the same spirit, the UK CMA looks confidently to the existing UK and EU competition law frameworks as being capable of dealing with the abuse of dominance by online platforms see Competition and Markets Authority (2015), para. 33.
[87] See Chirita (2014) 283.
[88] See European Data Protection Supervisor (2014), para. 2.2.10.
[89] See Evans and Schmalensee (2011) 17, offering several examples from residential property, securities, TV, media, operating systems, games to cards; on two-sided online advertising, see Rochet and Tirole (2003) 1; on critical features of two-sided markets, such as idiosyncratic matching and inefficient rationing, see Hermalin and Katz (2016).

it comes to Google's search-engine,[90] whose share of the general internet search exceeds 90 per cent of the market. Empirical research on Internet search advertising found that this market allows for 'very precise' targeted advertising.[91] Targeted advertising is often associated with privacy intrusion by advertisers,[92] but could also go beyond that to interrupt the online experience of consumers.[93]

Without disregarding the incontestable direct benefits derived by users from Google's online search-engine platform,[94] the giant extracts nearly $74.5 billion in revenues, with a 17 per cent increase from advertising.[95] In *Vidal-Hall v Google Inc.*,[96] there is evidence that in 2011, Google extracted $36.5 billion from advertising. Google's mysterious way of gaining profits moves away from a 'magic circle'[97] to a commercial platform where users' searches are returned with featured ads. Advertising is supported by a bulk of data collected from Google's users. This has led Newman to describe Google's advertising as 'a monument to converting privacy into a modern currency (…) based on particular user demographics and backgrounds that the advertiser may be looking for'.[98] Another commentator expressed Google's potential sale of users' data as a privacy derivative, nicknaming it *Googlestroika* to add a public sense of state surveillance.[99] In sharp contrast, two notable commentators regard 'the monetization of data in the form of targeted advertising' as being pro-competitive and not harmful, but rather, 'economically-rational, profit-maximizing behaviour'.[100] However, Evans, who has done pioneering work on 'matching advertising'[101] to consumers, took a more nuanced stance. While the efficacy of online targeted advertising in reducing marketing costs is incontestable, Evans recognised that the collection and analysis of data 'raises difficult issues concerning the expectation of privacy'.[102] The analysis of targeted advertising, which has been made the subject of another economic analysis,[103] has also highlighted the pro-competitive benefits of targeted advertising. However, it raised the alarm over targeting large amounts of data about consumers. It is believed that targeted advertising will often lead to highly concentrated market structures, such as Google and Facebook.[104] Ultimately, privacy could trigger the enactment of regulations that might be capable, or not, of limiting targeted advertising.[105]

The next section will prove that Google is not alone in engaging in anti-competitive misuse of personal data. First, however, it is argued that the new information economics proves incredibly costly for

[90] See EU Commission (2015); Chirita (2015) 115; for the contrary opinion that Google is only dominant in a 'populist', rather than rigorous, antitrust sense, see Wagner von Papp (2015) 641.
[91] See Rutz and Bucklin (2011); on auction sales of sponsored links in keyword searches, see Edelman, Ostrovsky and Schwartz (2007) 242.
[92] See Tucker (2012) 326.
[93] ibid 327.
[94] On search-engines as a multi-sided platform, see Hoppner (2015) 356; Lianos and Motchenkova (2013) 419.
[95] Alphabet Investor Relations (2016).
[96] Para. 6.1. of the Appendix to the judgement in *Vidal-Hall v Google Inc.* [2015] EWCA Civ 311 (27 March 2015).
[97] Chirita (2010) 111.
[98] Newman n 13; Newman (2014) 3.
[99] Muth (2009) 337.
[100] See Sokol and Comerford, 4; Lerner (2014).
[101] That general advertising to a wider audience has to sort out a 'matching' problem by delivering multiple advertisements to a large number of consumers, see Evans (2009) 43.
[102] ibid 38.
[103] Bergemann and Bonatti (2011) 438.
[104] ibid.
[105] Evans (2009) 52; for the contrary opinion, see Campbell, Goldfarb, and Tucker (2015) 47, who demonstrate that privacy regulation could help entrench digital monopolies.

consumers since online service users possess only imperfect information[106] about the real price to be paid in exchange for the freely available digital platform. This chapter agrees with Stiglitz's theory of economic inequality in the sense that 'increasing information asymmetry feeds increasing economic inequality'.[107] In particular, this author argues that the above mentioned consumers, through their lack of information about their personal, behavioural, experience, and authentication data with which they pay their dues for the use of online services, perpetuate such economic inequality inflicted through price discrimination. Advertisers increasingly use techniques that target online customers based on data collected from their service partners, namely, individual preferences, physical location, and other characteristics.[108] Ultimately, while targeted advertising increases corporate profits for all platforms, another study points out that consumers could, but need not, become better off.[109]

The challenging side of the data misuse remains that, as the price for data is unknown to online service users, the demand, i.e. service, and supply, i.e. data, curves cannot intersect each other in equilibrium. According to Salop and Stiglitz, in such a scenario, any economic analysis of efficiency becomes obsolete.[110] As rightly foreseen by Ohlhausen and Okuliar,[111] it represents a clear departure from the conventional analysis of market price equilibrium. It is advanced that, despite its legal connotation, privacy denotes all kinds of personal data surrounding a potential buyer, who is misled into accepting a much higher price than the actual, real price that could have been paid if the seller had not known about that data.

Speculations about financial status, preferences, or personal choice offer the chance of going up or down for select categories of buyers. Known as 'data mining',[112] targeted advertising allows sellers to make differential advertising offers to a particular group of customers based on useful correlations derived from their past online behaviour or user location. As has been suggested, it would be useful to study empirically the role of social connections and geographic proximity in shaping preferences and consumer purchasing.[113]

The Wall Street Journal found evidence to suggest that 'areas that tended to see the discounted prices had a higher average income than areas that tended to see higher prices'.[114] The emerging price discrimination relied on the assumption that poor areas have fewer retail options available locally so that higher prices can easily exploit online retail consumers. This kind of online discrimination experienced by consumers from poorer neighbourhoods has recently been acknowledged by the US Federal Trade Commission.[115] The FTC's report was endorsed by

[106] Also, see Tucker (2014) 546, who identified the need to conduct empirical work on the extent of information asymmetries between consumers and firms in this industry.
[107] Stiglitz (2002) 460, 479.
[108] Newman (2014) 853 highlighting Google's ascension through similar advertising techniques that rely on Google's available user data.
[109] See Johnson (2013) 140.
[110] Salop and Stiglitz (1982) 1121. Recently, Edelman developed an economic model suitable for online platforms, suggesting that competition between intermediaries intensifies distortions, see Edelman (2015) 1283.
[111] Ohlhausen and Okuliar (2015).
[112] Newman (2014) 868.
[113] Einav and Levin (2014) 12430891.
[114] Wall Street Journal (2012).
[115] US Federal Trade Commission (2016) 11.

Commissioner Ohlhausen given the impact of big data on 'low-income, disadvantaged, and vulnerable consumers'.[116]

Unfortunately, there remains a persistent research gap in the empirical literature on online price discrimination. One year ago, the UK Competition and Markets Authority had usefully commissioned its first research report on the commercial use of consumer data, albeit in selected sectors of the economy, such as motor insurance, clothing retail, and games apps.[117] Although limited in scope, the report attempted to provide insights into consumer data, in particular, personal and non-personal data, such as pseudonymous and aggregate data. It also looked into the ways in which consumer data is being collected, namely, inferred, explicitly declared, or observed through users' interaction. Furthermore, this report sheds light on the current use of behavioural data. A previous study had identified that even 'unstructured' data extracted from individuals' browsing history could reveal relevant economic interests,[118] from which wealth status could also be inferred.

Overall, there are too many data-driven platforms available which are capable of sharing economically relevant data for the purpose of price discrimination. This has recently led one commentator[119] to suggest the emergence of serious accountability issues due to the fact that it will often be impossible to identify any leak of personal data. Big corporations like Google, Facebook, Yahoo!, and Microsoft have used a combination of big data predictive economics models with sophisticated mechanisms to study individual decisions with reference to key variables.[120] Einav and Levin agree that an enormous amount of data increases the likelihood of identifying which ads to show.[121]

Professor Klock had critically captured the perils of price discrimination, i.e. 'where one set of consumers is unknowingly paying more for the same product than others' as being 'a clear sign of failure in the marketplace that calls for governmental intervention'.[122]

On the basis of the arguments exposed earlier, this chapter first argues that online price discrimination contributes to higher corporate profits and economic inequality. Second, it argues that competition policy intervention is therefore needed to curb this economic inequality that generates a false impression that a few digital giants are competing on the merit of their 'highly innovative' data-driven products and performance. Third, this chapter argues that dominant digital monopolies compete on the basis of their online users' personal, economically relevant, and sensitive bulk of collected data. This innovative IT engineering, which has already won solid corporate profits, should no longer pass unobserved by competition authorities' investigations.

Finally, the negative effects of price discrimination on consumers have recently been acknowledged by the OECD, namely that

'consumers may be increasingly facing a loss of control over their data, and their privacy; they are confronted with intrusive advertising and behavioural discrimination, and are ever more locked-in to the services upon which they rely'.[123]

---

[116] See Separate Statement of Commissioner Ohlhausen (2015).
[117] DotEcon & Analysys Mason (2015).
[118] Einav and Levin (2014) 12430891.
[119] See Nehf (2016)
[120] Einav and Levin (2014) 12430896.
[121] ibid 12430895.
[122] See Klock (2002) 317.

6. A Comparative Assessment of Empirical Case Studies of Privacy

The following section is dedicated to exploring how privacy policies work in practice for consumers of online products or services. In the economic literature, it has already been advanced that there is no empirical basis which could demonstrate that 'large online platforms are likely to collect more data', including more sensitive data,[124] than their smaller counterparts. This section seeks to investigate the privacy policies of four major online platforms, namely, Microsoft, Google, Facebook, and Linked-In. It will primarily focus on the categories of data being collected, the sharing of such data, consent, and disclosure. As during the writing of this chapter it became clear that smaller competing online platform were also important, Instagram, Snapchat and Whisper are also included. Rather than based on any other criterion, due to this author's personal preference, Google tops the table below, which presents an overall picture of the findings.

Privacy Policies	Collected Data	Data Sharing with	Disclosures	Consent
Google	i. **personal data** until June 2015 & **personal search queries**; ii. **behavioural** data; iii. **experience** data, i.e. cookies, Google Analytics tracking via DoubleClick; iv. **economically relevant** data, i.e. interactive advertising;[125] v. **unique device identifiers** ✓ **Authentication**	**thirds**: i. companies, organisations or individuals; ii. **aggregated data** with publishers, advertisers or connect sites.	a) meeting legal requirements or a governmental request; b) investigating violations; c) detecting or preventing fraud, security or technical issues; d) protecting own interests or that of its users.	Required. **Opt-in** for (i) sensitive personal data; (ii) combining DoubleClick cookies with personal authentication.
Microsoft Windows 10	i. **personal** data until Jan. 2016; ii. **behavioural** data; iii. **experience**, i.e. cookies, incl. targeted advertising; iv. **device-specific** (IT) ✓ **Authentication**	i. **thirds** until Jan 2016; ii. controlled affiliates, subsidiaries, vendors.	a) legal disclosure; b) users' protection against spam, fraud; c) its own security interests.	Required. **Opt-out** for 'interest-based advertising'.
Facebook	i) **personal** data; ii) **experience** and **usage data**, i.e. visualised content, personal engagement, user frequency and duration; iii) specific **location data**; iv) **behavioural data** from third party advertisers through 'relevant ads on and off' service.	i) companies that are part of Facebook; and ii) integrated third party apps, websites or other services, including third party advertisers.	a) legal request, i.e. search warrant, court order or subpoena; b) where the law so requires , incl. from jurisdictions outside of the US; c) detecting, preventing and addressing fraud or other illegal activity; d) its own protection or that of others; e) preventing death or imminent bodily harm.	**Permission required** for sharing personally identifiable data with third party advertisers or analytics partners; **No consent** for: i) targeted advertising and aggregated data transfer, i.e. age, sex, location, and personal preference, to vendors, service providers and business partners; ii) transferring personal data to countries outside the EEA.
Instagram	i) **personal data;** ii) **analytics** of personally non-identifiable **data** , i.e. traffic,	i) personal, experience, local and behavioural data with **businesses**	a) in response to a legal request, i.e. search warrant, court order or	**Consent** for i) renting or selling data to third parties;

[123] OECD (2016), 29.
[124] See Lerner (2014), para. 85.
[125] Cookies are small text files place on users' device to help Microsoft collect data and store its users' preferences and settings, to sign-in, provide targeted advertising, combat fraud and to analyse service performance.

	usage, interactions; iii) **experience data** , i.e. cookies, local storage; iv) **behavioural data** , i.e. serving ads; v) **location data**, incl. unique device identifiers; vi) **aggregated data**, i.e. total number of visitors, traffic and demographic patterns.	**that are legally part of the same group** and its affiliates; ii) experience and location data with **thirds**; iii) **anonymized data** for targeted advertisements and **aggregated data** with **others.**	subpoena; b) when the law so requires; c) detecting, preventing and addressing fraud and other illegal activity; d) protecting itself and its users; and e) preventing death or imminent bodily harm.	ii) transferring personal data to another jurisdiction.
Linked-In	i. **personal** data; ii. **experience** data, i.e. cookies; iii. **behaviour** data, i.e. targeted advertising; iv. **inferred** and **aggregated** data. v. **location** data.	i) **affiliates**; ii) **third parties**, i.e. publishers and advertisers; No renting or selling of personal data.	a) where permitted by law; b) reasonably necessary to comply with a legal requirement; c) compulsory disclosures; d) responding to claims of violations; e) its own interest or that of its users.	i) **assumed consent** for service functionality; ii. **separate permission**, ie **opt-in consent** for personal use of cookies by third party advertisers and ad networks; iii. **opt-out** from target advertising only, but not from general advertising; iv. **presumed consent**, i.e. express and voluntary acceptance of its user agreement.
Whisper	i. **Usage data;** ii. **location data**; iii. **behavioural data** to personalise user's experience; iv. **device-specific data** , i.e. unique device identifier; v. **experience data**, incl. previous URLs.	i) **other users** and **the public**; ii) other **nearby users** location data; iii) **vendors**, **consultants** and other **service providers**; iv) as a result of M&A; v) current and future **affiliates**, **subsidiaries** and other companies; vi) third parties: **aggregated data**.	a) in good faith, where it is necessary to comply with a law, regulation, legal process or governmental request.	i. with consent, i.e. location; ii. no consent for **behavioural or aggregated data**, incl. for analytics and advertising. iii. **opting out** of having web browsing used for behavioural advertising. iv. on Android, mobile, 'Limit Ad Tracking' feature to **opt out of interest-based ads**.

6.1. A Comparative Assessment and Classification of the 'Big Data' Collection

This chapter proposes the following classification of big data on the basis of a comparative analysis of the data collected by multi-sided online platforms. First, this chapter argues that behavioural, usage and content, experience, technical, and location data are all sub-categories of personal data, albeit indirectly, compared to more direct, or highly sensitive, personal data. Aggregated data belong to the category of inferred data from any of the above. Second, the chapter wishes to advance that there is a real danger stemming from the abuse of objectively established commercial justifications of improving security, functionality, or service experience through recent attempts to authenticate users for targeted advertising. The latter fully exploits users' economic behaviour and trust, and their lack of education and awareness. Third, this chapter recognises exploitative abuse based on behavioural economics as a competition issue while viewing the remaining abuse as belonging to consumer law. The author also recognises that economists could still be irritated by the third proposition, as they need to look at all the complexities of a case, and in doing so, they rarely consider the artificial

division of competition, consumer, or data protection laws. In the same spirit, a recent EU soft law communication acknowledges that online platforms are incredibly complex, being subject to competition and consumer law, personal data, and marketing law, and to the Digital Single Market's freedom for 'data-driven innovation'.[126]

6.1.1 Direct Personal Data

Up to January 2015[127] and June 2015,[128] Microsoft and Google collected personal data from their users of Windows 10 and search-engine respectively, such as name and email. However, Google encrypts many of its services, restricting access to personal data to its own employees, contractors, and agents only. Linked-In collects personal data, such as email address book, mobile device contacts, or calendar, in order to offer its users a 'personalised and relevant experience'. Facebook collects personal data used by its users for signing up. Owned by Facebook since September 2012, Instagram also collects personal data, i.e. email address. Surprisingly, Snapchat collects personal data, ie email address, phone number, and even date of birth. Only Whisper does not collect personal data, as a username is different from the user's real name.

6.1.2 Highly Sensitive Personal Data

Google claims that it did not use cookies or similar technologies for sensitive data, i.e. race, religion, sexual orientation, or health. However, its users cannot disable cookies if Google's services are to function properly.

6.1.3. Behavioural Data

Microsoft collects behavioural data, such as users' preferences and interests, while Google collects similar data, which could reveal 'more complex things' and have an economic significance, i.e. most useful ads, people who matter most, or 'likes' for YouTube videos. Similarly, Linked-In collects behavioural data 'to learn about' its users' interests, while Whisper collects the same data[129] intended 'to personalize user experience'.

6.1.4 Content and Usage Data

Microsoft collects usage data, such as browsing and search history, while Google collects logging data about how often users made use of its search engine and their own personal search queries. In addition, Google now stores personal data from its users' browser, including HTML, and application

[126] EU Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Online Platforms and the Digital Single Market COM (2016) 288/2, paras 5 and 11.
[127] See Microsoft's Privacy Statement of January 2015.
[128] See Google's Privacy Policy, last modified, 30 June 2015.
[129] The data includes time, pages, whispers viewed, and interactions.

data caches. Even more invasive of its users' privacy is the fact that Google combines personal data from one of its multiple innovative services with that from another. Likewise, Facebook collects the content provided when individuals use its service, including any messages and communications, the location and data of a photo, and usage data, such as the types of visualised content, personal engagement, frequency, or duration.

According to its privacy policy as of January 2013, Instagram collects content data, i.e. photos, comments, and communications, and usage data, including browsing. The latter are passed on to third parties to 'personalize' content and ads. Instagram uses third party analytics to measure service traffic and usage trends, like URLs, number of clicks, interactions, and viewed pages. However, Instagram claims that its analytics data are not used to identify a particular user. Snapchat also collects usage data, namely, social interactions, communications, messages, and content. According to its latest privacy policy of March 2016, Whisper collects usage data, i.e. content, publicly available replies and chat messages, and interactions.

6.1.5 Technical versus Authentication Data

Microsoft, Google, and Snapchat collect device-specific data, while Facebook collects device identifiers. However, while Microsoft collects IT data about device configuration, Google collects more comprehensive data, including the operating system, unique device identifiers, mobile network, and phone number. Since March 2016, Google associates the unique device identifier or phone number with a user's account. Likewise, Linked-In, Instagram, Snapchat, and Whisper collect mobile device identifiers for data authentication, which for Snapchat, includes advertising and unique device identifiers.

6.1.6. Location versus Authentication Data

Microsoft and Google collect location data. However, Google collects data that can uniquely identify a user's actual location, such as IP address, GPS, Wi-Fi access points, and mobile towers.[130] In contrast, Linked-In collects location data for targeting its users with local jobs or for the purpose of fraud prevention and security. Facebook, Instagram, and Snapchat collect location data, including specific (Facebook) or precise (Snapchat) location data. Finally, Whisper collects past and present location data or at least an approximate geographic location.

But why would anyone track users' locations? In the US *re Aaron's, Inc* case,[131] the franchisees of a rent-to-own dealer of leased computers used computer software to track customers' locations, capture webcam images, and activate keylogging software to steal login credentials for email accounts and financial and media sites. Evans suggested that, compared to larger companies, individuals browsing from home are most exposed to targeted advertising, as they maintain a unique

[130] Users' identification through cookies applies to many of Google's innovations, such as Places, Travel, Product Search, Chrome, Maps, Scholar, YouTube, Talk, Gmail, Google+, Android etc.

[131] FTC, *Re Aaron's Inc.*, no C-4442 [2014], available at https://www.ftc.gov/enforcement/cases-proceedings/122-3256/aarons-inc-matter.

IP address over time.[132] Bergemann and Bonatti advanced an insightful economic model of profitability based on IP address tracking by online advertisers.[133]

6.1.7 Objectively Justifiable Personalised Service Experience versus Authentication Data

The majority of the corporations under review, namely, Microsoft, Google, Linked-In, Snapchat, and Whisper, collect experience data, store users' preferences and settings and, eventually, authenticate them for fraud detection. Microsoft last updated its privacy policy in January 2016. It now claims to collect data to operate effectively and provide its users with the best service experience. While the latter purpose is entirely and objectively justifiable, Microsoft aims not only to improve but also to personalise its users' experience. The latter seems problematic, as any attempt to personalise data will, in turn, compromise privacy.

Google collects cookies, which uniquely identify its users' browser, local web storage, and data caches. At a first glance, this is objectively justifiable for improving services for users, namely, by showing them more relevant search results or making the sharing with other users quicker and easier. For this purpose alone, Google collects a vast array of information that figures out 'basic stuff', eg spoken language. However, there are blurring boundaries between improving users' experience and authenticating them. Apart from this, Google pursues its own objective commercial interests, namely, to provide, maintain, protect, and improve its services and develop new ones, and to protect its own users. Similarly, Linked-In collects objectively justifiable data from users to improve their experience and increase their security. Instagram collects experience data, including local storage. Snapchat collects unique advertising identifiers about its users' online activities. However, it claims that such data is used to monitor and analyse trends and usage and to personalise the service. Finally, Whisper uses similar tracking technologies, including the URL a user had visited before navigating to its service.

The Recent Report of the German Monopolies Commission reached a similar conclusion, namely that social platforms of this kind display an incentive to acquire larger amounts of personal data.[134] This goes beyond what is objectively necessary for ensuring the proper functioning of the platforms.

6.1.8 Targeted versus General Advertising

Microsoft uses personalised data to help make commercial ads more relevant to its users. Google's latest privacy policy of March 2016 acknowledges that the corporation collects usage data about its own advertising services, such as views or interactions with commercial ads. Most importantly, through cookies, Google also stores economically relevant data about its users' interaction with the advertising services offered by Google's partners or features that may appear on other sites. Analytics data is corroborated with advertising services using DoubleClick to generate further data about visits to multiple sites. Google Analytics is yet another powerful tool for businesses and site owners to analyse the traffic to their websites and apps.

[132] See Evans (2009) 42.
[133] Bergemann and Bonatti (2001) 438.
[134] Monopolies Commission (2015).

Similarly, Linked-In collects behavioural data to 'serve' general advertising, through various advertising technologies, including web beacons, pixel, tags, or cookies. Furthermore, Linked-In makes use of targeted advertising based on its users' public profile or inferred data; usage, including search history, read content, following activity, participation in groups, visited pages, and so on; and, most importantly, third parties, such as advertising partners, publishers, and data aggregators. More specifically, advertisers receive the URL of a user's current page when the user clicks on an ad.

Facebook collects behavioural data from third party advertisers when its users visit or use third party websites or apps or when they interact with third party partners. Facebook aims to improve its advertising to existing users to show them 'relevant ads on and off' its service and to measure the effectiveness and reach of such ads. Instagram uses similar technologies 'to serve ads' by advertisers and other partners.

6.1.9 Written Email and Voice Data

The following 'reassuring' disclaimer, which is used by Microsoft, is actually worrying: 'we do not use what you say in email, chat, video calls or voice mail, or your documents, photos or other personal files to target you'. However, Google collects data about the time, date, and duration of calls. Paragraph 1.8 of Linked-In's privacy policy on the use of cookies assumes that, by visiting its service, users consent to the placement of cookies and beacons not only in their browser, but also in HTML-based emails. A recent empirical study has proved how invasive of privacy is the automated email content analysis by Facebook, Yahoo, and Google.[135]

6.1.10 Aggregated Data

For commercial purposes, Instagram monitors metrics, such as total number of visitors, traffic, and demographic patterns, i.e. aggregated data. This is in contrast to diagnosing or fixing technology problems. Also, Google shares aggregated, non-identifiable, data publicly and with third parties, such as publishers, advertisers, or connected sites. Facebook shares with third parties data about the reach and effectiveness of their advertising as well as aggregated data. For example, Facebook passes on to third parties data about the number of ad views or demographic data based on its users' age, sex, location, and personal preference. However, Facebook transfers such data to vendors, service providers, and business partners in order to measure the effectiveness of their ads. Instagram also shares aggregated data which can no longer be associated with a particular user. Similarly, Snapchat shares aggregated or 'de-identified' data with third party advertisers. Finally, Whisper shares aggregated data with vendors, consultants, and other service providers.

6.2. Data Sharing

[135] See Strahilevitz and Kugler (2016), 20.

Data sharing is possible both inside and outside of an online platform. The former could be as harmful as the latter in the case of a merger or acquisition.

6.2.1 Inside Sharing of Data

Most corporations share personal data with their controlled affiliates (Linked-In, Whisper) and subsidiaries (Microsoft, Whisper), other companies that are part of the same group (Facebook, Instagram and Snapchat), or under common control and ownership (Snapchat). Logically, Instagram shares personal content and usage, experience, and local and behavioural data with Facebook. Snapchat shares similar data with the Snapchat family of companies.

6.2.2 Outside Sharing of Data

Until January 2016, Microsoft shared its users' personal data with third parties, including vendors. Google did the same with third party companies, organisations, or individuals. Linked-In shares personal data with third parties, while Facebook shares service content, like posts or shares, with integrated third party apps, websites, or other services, including advertisers. Instagram shares experience and location data with third parties. It shares anonymized data with third parties in order for them to deliver targeted advertisements. Similarly, Snapchat shares personal data with third parties, which may include service providers, i.e. for quality of service; sellers, i.e. providing goods; and partners, i.e. functionality of service, or as a result of a merger or acquisition. Snapchat users themselves provide personal data to third parties simply by clicking on their links or search results. Third parties may use personal data collected by Snapchat to deliver targeted advertisements, including third-party websites and apps. Whisper also shares similar data with the public. In contrast, the recipient of a chat message could share its content to others. Location data is shared with other nearby users.

On the basis of the above, this chapter identifies that data sharing to third parties, mostly advertisers, is common practice. Linked-In is the only platform to have placed a rather obvious disclaimer according to which it does not 'rent or sell' personal data that its users have not posted on Linked-In.

6.3. Consent

6.3.1 Subject to Consent

Microsoft and Google claim to share personal data subject to their users' consent. Linked-In shares similar data subject to consent in order to carry out instructions by users, provide functionality, protect consumer rights, or comply with laws. Surprisingly, Instagram claims to not 'rent or sell' data to third parties without its users' consent, while Snapchat collects with-consent phonebook data and photos. Whisper also shares with-consent location data.

6.3.2 Opt-In (Explicit) Consent

Microsoft users are already signed in to receive targeted advertising without any prior consent. Google requires opt-in consent for sharing sensitive personal data. Since March 2016, Google requires opt-in consent for combining DoubleClick with personally identifiable data. Likewise, Linked-In requires 'explicit' opt-in consent for personal data collected directly by third party advertisers through cookies.

6.3.3 Presumed Consent

Linked-In presumes that valid consent has been given to the use of beacons and other advertising technologies. It assumes that, by providing personal data, Linked-In users have 'expressly and voluntarily' accepted the terms and conditions of its Privacy Policy, thereby 'freely accepting and agreeing' to such data processing. One disclaimer mentions that supplying any information deemed to be sensitive by applicable law is entirely voluntary. Another disclaimer warns Linked-In users not to become members if they have any concerns about providing data.

6.3.4 Explicit Consent or Special Permission

Google promises its users not to reduce their rights under its current privacy policy without their explicit consent. But isn't it too late for getting such consent, since Google has already collected plenty of information about its users, namely, usage data, preferences, messages, photos, videos, browsing history, map searches, documents and other Google-hosted content? Under these circumstances, could it still be argued that raising awareness about Google's search-engine and educating its users as consumers about their online behaviour would suffice to address the abuse of data with given, but less informed, consent? Most users can barely understand the legal implications of such explicit consent.

Linked-In requires 'separate permission' for sharing personal data with third party advertisers or ad networks for advertising. Facebook requires similar permission for sharing personally identifiable data, ie name or email address, with third party advertisers or measurement or analytics partners.

6.3.5 Opt-Out Choice

Microsoft offers an 'opt-out' choice, informing its users to visit Microsoft's opt-out page. According to Linked-In's privacy policy of October 2014, in particular, its second commitment, 'If you wish to not receive targeted ads from most third party companies, you may opt-out by clicking on the AdChoice icon in or next to ad'. However, according to its third commitment, 'This does not opt any user out of being served advertising.' Linked-In's users are empowered to opt out of targeted ads only. They can opt out if they no longer wish their online behaviour to be tracked on third party sites. In contrast, Whisper users can opt out of having their web browsing information used by participating companies

for behavioural advertising purposes. On Android mobile, users have to choose the 'Limit Ad Tracking' feature to opt out of interest-based ads.

6.3.6 No Consent

Obviously, no consent is required from Linked-In for its users' public posts. In contrast, Whisper does not require consent for sharing behavioural or aggregated data with third parties, including for analytics and advertising.

Apart from this, there is further scope for trouble because Linked-In processes personal data outside the country where its users live. Facebook may also transfer personal data to countries outside the European Economic Area. Likewise, Instagram and its affiliates or service providers may transfer personal data across borders to another jurisdiction, which has different data protection laws. Snapchat may also transfer personal data to jurisdictions other than the United States.

Finally, this chapter identifies as common practice users agreeing to give consent on a 'take-it-or-leave-it' basis, without having any viable alternative to the use of cookies. Otherwise, the service in question could not work properly.

6.4. Disclosure of Data

The most commonly known ground for outside disclosure is where personal data is necessary to comply with any applicable law (Microsoft, Google, Whisper), rule or regulation (Google, Snapchat, Whisper); requirement or valid legal request (Instagram, Snapchat), such as a search warrant (Facebook, Instagram), civil or criminal subpoenas (Linked-In, Facebook, Instagram), court orders (Facebook, Instagram) or other compulsory disclosures (Linked-In) or to respond to a valid legal process (Facebook, Whisper) from competent authorities, including from law enforcement or other government agencies (Microsoft, Google, Whisper) and from jurisdictions outside of the United States (Facebook, Instagram); in good faith, where it is permitted by law (Linked-In); for the investigation of potential violations (Google, Linked-In, Snapchat); to enforce a privacy policy or user agreement (Linked-In); to protect customers by preventing spam (Microsoft, Google) or to detect or address fraud (Microsoft, Google, Facebook, Instagram, Snapchat); to prevent loss of life or serious injury (Microsoft); to prevent death or imminent bodily harm (Facebook, Instagram); to operate and maintain product security (Microsoft, Google), technical issues (Google), or safety (Snapchat); and to protect its own rights and property (Microsoft, Snapchat), interests, and users (Google, Linked-In, Facebook, Instagram, Snapchat) or the public (Google).

Finally, Instagram uses an alarming disclaimer that states that it cannot ensure the security of any transmitted information or guarantee that such information is not accessed, disclosed, altered, or destroyed.

7. A Response from Practice: *Vidal-Hall v Google Inc* [2015] EWCA

In *Vidal-Hall v Google Inc*,[136] the claimants did not consent to the use of cookies on their Apple Safari browser. Advertisers used aggregated data about the claimants' browsing experience to target them via the DoubleClick advertising service. As a result of this targeted advertising, personal data was shared with third parties. On appeal, the Royal Court of Justice established a tortious liability for 'misuse of private information'. Similar to this chapter's advancement of abuse of personal data by digital monopolists, *Vidal-Hall v Google Inc.* has significant implications for the misuse of personal data through the online browsing activities of individuals. While the Court welcomed the possibility of awarding damages for distress in the absence of proof of a pecuniary loss, civil litigation of this kind demonstrates the risks to the consumer and to data protection laws if they are left unaddressed by competition policy intervention. The tortious measure could to do justice solely in individual law suits.

This case represents a landmark ruling. It recognised the 'misuse of private information' as an 'invasion of privacy'.[137] Unfortunately, when it interpreted Directive 95/46/EC, the Court suggested that the directive aims to protect 'privacy rather than economic rights'.[138] The same could be said about the reference to the misuse of 'private information', rather than of personal data. The High Court's Justice Tugendhat had previously recognised that browsing information is, indeed, personal data, and that it could have the potential to identify the claimants 'as having the characteristics to be inferred from the targeted advertisements by third parties viewing the claimants' screens'.[139]

The Royal Court of Justice recognised that 'web traffic surveillance tools make it easy to identify the behaviour of a machine, and behind the machine, that of its user'.[140] The Court went on to distinguish between two categories of personal data: on the one hand, direct personal data, including detailed browsing histories, and on the other, the data derived from the use of the DoubleClick cookie.[141] As the latter includes a unique identifier, indirectly inferred data could have enabled the former, i.e. direct personal data, to be linked to an individual device user. In the Appendix to this ruling, there is evidence of the wealth of personal data collected by Google via DoubleClick, including economically relevant data, such as shopping habits, social class, and financial situations, but also many others, like racial or ethnic origin, health, or sexual interests.[142] Unfortunately, Safari browsers have no 'Opt Out' cookies available that would enable their users to sign off from tracking and targeted advertising.

The Court considered that 'targeted advertising is inevitably revelatory as to the browsing history of a particular individual'.[143] Given the limited appetite for awarding an 'extremely high' figure of damages for distress, ie £1.2 million, LJ McFarlane dismissed the appeal to the Supreme Court. The ruling also followed the US developments in private litigation. The FTC had settled with Google a civil penalty of $22.5 million because of the misrepresentation to users of the Safari browser that it would not use cookies or serve targeted advertisements to them.[144]

---

[136] *Vidal-Hall v Google Inc.* [2015] EWCA Civ 311 (27 March 2015); on appeal from the High Court (QB) The Hon Mr Justice Tugendhat [2014] EWHC 13 (QB).
[137] Ibid, paras 19 and 23 for the recognition that courts of equity have afforded protection to the misuse of private information via the breach of confidence route.
[138] Ibid, para. 77.
[139] Ibid, para. 111.
[140] Ibid, para. 114.
[141] Ibid, para. 115.
[142] Ibid, para. 8.1. to 8.4.
[143] Ibid, para. 128.
[144] Ibid, para. 140.

8. Conclusions

The above study of the privacy policies operated by some digital companies has revealed the many inter-related purposes of the collection and processing of the various categories of personal data. It identified that digital giants have, indeed, pursued nearly identical business models based on corporate gains from targeted advertising and exploitation of consumers as online users of a particular service platform. Indeed, the processing of certain categories of data is objectively justifiable for making the service in question work better for its users. However, other categories of usage, content, and behavioural data tend to be rather excessively processed for the benefit of commercial advertising by third parties. Knowing a consumer's usage, frequency, preferences, and choices builds up a picture of their prospective economic behaviour. It disempowers such online consumers from any natural status of rational buyers while making them more vulnerable vis-à-vis online sellers or retailers. Giving consent and opting-in or out remain useful compliance tools for corporations that seek to stay safe from data protection rules. But can they also remain so before competition authorities?

References

Acquisti A. and Varian H.R. (2005), Conditioning prices on purchase history, Marketing Science 24
Albors-Llorens A. (2014), Competition and Consumer Law in the European Union: Evolution and Convergence, Yearbook of European Law 33
Alphabet Investor Relations (2016), Alphabet Announces Fourth Quarter and Fiscal Year 2015 Results, press release (1 February)
Armstrong M. and Vickers J. (2001), Competitive Price Discrimination, Rand J. of Econ. 32
Autorité de la concurrence and Bundeskartellamt (2016), Competition Law and Data, available at http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf
Baker J.B. (2003), Competitive Price Discrimination: The Exercise of Market Power without Anticompetitive Effects, Antitrust Law J. 70
Barr-Gill O. (2012), Seduction by Contract: Law, Economics, and Psychology in Consumer Markets, Oxford University Press
Beale H. (2002), Legislative Control of Fairness: The Directive on Unfair Terms in Consumer Contracts, in J. Beatson / D. Friedmann (eds) Good Faith and Fault in Contract Law, Oxford, Clarendon Press
Bellamy and Child (2013), European Union Law of Competition, in V. Rose/D. Bailey (Eds.), 7th ed., Oxford University Press
Bergmann D., Brooks B. and Morris S. (2015), The Limits of Price Discrimination, American Econ. Review 105
Bergemann D. and Bonatti A. (2011), Targeting in advertising markets: implications for offline versus online media, RAND J. of Econ. 42
Bigwood R. (2003), Exploitative Contracts, 1st ed., Oxford University Press
Bundeskartellamt (2016), press release, Bundeskartellamt initiates proceedings against Facebook on suspicion of having abused its market power by infringing data protection rules
Bundeskartellamt (2016), Working Paper: The Market Power of Platforms and Networks (June)
Campbell J.D., Goldfarb A., and Tucker C. (2015), Privacy Regulation and Market Structure, J. of Econ. & Management Strategy 24
Chirita A.D. (2010), Undistorted, (Un)fair Competition, Consumer Welfare and the Interpretation of Article 102 TFEU, World Competition Law & Econ. Review 33
Chirita A.D. (2014), A Legal-Historical Review of the EU Competition Rules, Int. and Comparative Law Quarterly 63
Chirita A.D. (2015), Google's Anti-Competitive and Unfair Practices in Digital Leisure Markets, Competition Law Review 11
Committee of Economic and Monetary Affairs (2014), Hearing of Margrethe Vestager (2 October)
Competition and Markets Authority (2015), Written Evidence (OPL0055) to the House of Lords' Inquiry on Online Platforms and the EU Digital Single Market, available at https://www.publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/129.pdf
Cooper E.H. (1977), Price Discrimination Law and Economic Efficiency, Michigan Law Review 75
DotEcon & Analysys Mason (2015), The Commercial Use of Consumer Data A research report for the CMA, available at
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf
Edelman B. (2015), Does Google Leverage Market Power through Tying and Bundling, J. of Competition Law and Econ. 33
Edelman B. (2015), Price Coherence and Excessive Intermediation, Quarterly J. of Econ. 130
Edelman B., Ostrovsky M. and Schwartz M. (2007), Internet Advertising and the Generalized Second-Price Auction: Selling Billions of Dollars Worth of Keywords American Econ. Review 97
Einav L. and Levin J. (2014), Economics in the Age of Big Data, Science 346
European Commission (2015), Statement by Commissioner Vestager on antitrust decisions concerning Google, 15/4785

European Data Protection Supervisor (2014), 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, available at https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf
Evans D.S. (2009), The Online Advertising Industry: Economics, Evolution, and Privacy, J. of Econ. Perspectives 23
Evans D. and Ezrachi A. (2015), Witness Statement to the House of Lords' Inquiry on Online Platforms and the EU Digital Single Market, available at https://www.publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/129.pdf
Evans D.S. and Schmalensee R. (2011), The Industrial Organization of Markets with Two-Sided Platforms, in: D.S. Evans (Ed.), Platform Economics: Essays on Multi-Sided Businesses, Competition Policy Int.
German Monopolies Commission (2015), 68th Special Report on Competition Policy: Challenges of Digital Markets, available at
http://www.monopolkommission.de/images/PDF/SG/SG68/S68_volltext.pdf
Grunes A.P. and Stucke M.E. (2015), No Mistake about It: The Important Role of Antitrust in the Era of Big Data, Antitrust Source 12
Hayek F.A. (2002), Competition as a Discovery Procedure, Quarterly J. of Austrian Econ. 5
Heffetz O. and Ligett K. (2014), Privacy and Data-Based Research, J. of Econ. Perspectives 28
Hermalin B.E. and Katz M.L. (2016), What's So Special about Two-Sided Markets?, forthcoming in Economic Theory and Public Policies: Joseph Stiglitz and the Teaching of Economics, Columbia University Press.
Hermalin B.E. and Katz M.L. (2006), Privacy, Property Rights and Efficiency: The Economics of Privacy as a Secrecy, Quantitative Marketing and Econ. 4
Hoppner T. (2015), Defining Markets for Multi-Sided Platforms: The Case of Search Engines, World Competition 38
Johnson J.P. (2013), Targeted advertising and advertising avoidance, RAND J. of Econ. 44
Joyce D. (2015), Privacy in the Digital Era: Human Rights Online?, Melbourne Journal of Int. Law 16
Kadar M. (2015), European Union Competition law in the Digital Era, Zeitschrift für Wettbewerbsrecht 4
Kerber W. (2016), Digital markets, data, and privacy: competition law, consumer law and data protection, J. of Intellectual Property Law & Practice
Kessler F. (1943), Contracts of Adhesion – Some Thoughts about Freedom of Contract, Columbia Law Review 43
Klock M. (2002), Unconscionability and Price Discrimination, Tennessee Law Review 69
Lerner A.V. (2014), The Role of 'Big Data' in Online Platform Competition, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2482780
Lianos I. and Motchenkova E. (2013), Market Dominance and Quality of Search Results in the Search Engine Market, J. of Competition Law & Econ. 9
London School of Economics (2015), Online Platforms and the EU Digital Single Market, Written Evidence (OPL0054) to the House of Lords, the Select Committee on the European Union
Lynskey O. (2014), Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order, Int. and Comparative Law Quarterly 63
Lynskey O. (2014), The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: *Digital Rights Ireland*, Common Market Law Review 51
Lynskey O. (2015), Control over Personal Data in a Digital Age: *Google Spain v AEPD and Mario Costeja Gonzalez*, Modern Law Review 78
Market Watch (2012), Who Would Pay $5,000 to Use Google? (You) (25 January)
Martens B. (2016), European Commission, Joint Research Centre Technical Reports, An Economic Policy Perspective on Online Platforms

Max Planck Institute for Innovation and Competition (2016), Data Ownership and Access to Data, available at http://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016_08_16-def.pdf
McDonald A.M. and Cranor L.F. (2008), The Cost of Reading Privacy Policies, Journal of Law and Policy for the Information Society, 17
Morgan J. (2015), Great Debates in Contract Law, 2nd ed., Palgrave
Muth K.T. (2009), Googlestroika: Privatising Privacy, Duquesne Law Review 47
Nehf J.P. (2016), Protecting Privacy with 'Heightened' Notice and Choice, in JA Rothchild (Ed.) Research Handbook on Electronic Commerce Law, Cheltenham, Edward Elgar
Newman N. (2014), The Cost of Lost Privacy, William Mitchell Law Review 40
Newman N. (2014), Search, Antitrust and the Economics of the Control of User Data, Yale J. on Regulation 30
O'Donoghue R. and Padilla A.J. (2006), The Law and Economics of Article 82 EC, 1st ed., Hart Publishing
OECD (2016), Big Data: Bringing Competition Policy to the Digital Era, DAF/COMP(2016)14
Ohlhausen M.K. and Okuliar A. (2015), Competition, Consumer Protection, and the Right [Approach] to Privacy, Antitrust Law Journal 80
Ohlhausen, M.K. (2015), Separate Statement, Big Data: A Tool for Inclusion or Exclusion (6 January)
Pasquale F.A. (2013), Privacy, Antitrust, and Power, George Mason Law Review 20
Posner R. (1980), The Economics of Privacy, American Econ. Review 71
Roberts A. (2015), Privacy, Data Retention and Domination: *Digital Rights Ireland Ltd v Minister for Communications*, Modern Law Review 78
Rochet J.C. and Tirole J. (2003), Platform Competition in Two-Sided Markets, J. of the European Econ. Association
Rutz O. and Bucklin R. (2011), From Generic to Branded: A Model of Spillover Dynamics in Paid Search Advertising, J of Marketing Research
Salop S. and Stiglitz J.E. (1982), The Theory of Sales: A Simple Model of Equilibrium Price Dispersion with Identical Agents, American Econ. Review 72
Schepp N.P. and Wambach A. (2016), Economist's Note on Big Data and Its Relevance for Market Power Assessment, 7.
Smith S.A. (2005), Atiyah's Introduction to the Law of Contract, Oxford, Clarendon Press
Sokol D. and R Comerford R. (2017), Does Antitrust Have a Role to Play in Regulating Big Data?, in R. Blair and D. Sokol (Eds.), Cambridge Handbook of Antitrust, Intellectual Property and High Tech, Cambridge University Press
Stigler J (1980), An Introduction to Privacy in Economics and Politics, J. of Legal Studies 9
Stiglitz J.E. (2002), Information and the Change in the Paradigm in Economics, American Econ. Review 92
Strahilevitz L.J. and Kugler, M.B. (2016), Is Privacy Policy Language Irrelevant to Consumers?, Chicago Coase-Sandor Institute for Law and Economics Working Paper no 776.
Tucker C. (2014), Social Networks, Personalized Advertising, and Privacy Controls, J. of Marketing Research 51
Tucker C.E. (2012), The economics of advertising and privacy, Int. J. of Industrial Organization 30
US Federal Trade Commission (2016), Report on Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues (January)
Vestager M. (2016), Competition in a Big Data World, Speech (18 January)
Wagner von Papp F. (2015), Should Google's Secret Sauce Be Organic?, Melbourne Journal of Int. Law 16
Wall Street Journal (2012), Website Vary Prices, Deals Based on Users' Information (24 December)
Wall Street Journal (2014) The Big Mystery: What's Big Data Really Worth? A Lack of Standards for Valuing Information Confounds Accountants, Economists (12 October)
Whish R. (2016), Article 102 and de minimis, Competition Law Journal
Whish R. and Bailey D. (2015), Competition Law, 8th ed., Oxford University Press