cerre Centre on Regulation in Europe
Improving network industries regulation

Consumer privacy in network industries

A CERRE Policy Report

Professor Pierre Larouche (CERRE and Tilburg Law and Economics Center, Tilburg University)

Professor Martin Peitz (CERRE and Mannheim Center for Competition and Innovation, University of Mannheim)

Dr. Nadya Purtova (Tilburg Institute for Law, Technology and Society, Tilburg University)

25 January 2016

Centre on Regulation in Europe (CERRE) asbl
Rue de l'Industrie 42 Box 16 - B-1040 Brussels - Belgium
Ph.: +32 (0)2 230 83 60 - Fax: +32 (0)2 23 0 83 70

Centre on Regulation in Europe

Improving network industries regulation

Table of contents

Centre on Regulation in Europe

Improving network industries regulation

About CERRE

Providing top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach;
- the widely acknowledged academic credentials and policy experience of its team and associated staff members;
- its scientific independence and impartiality;
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments and regulatory authorities, as well as at strengthening the expertise of the latter, since in many Member States, regulators are part of a relatively recent profession.

This study, within the framework of which this report has been prepared, has received the financial support of a number of CERRE members. As provided for in the association's by-laws, it has, however, been prepared in complete academic independence. The contents and opinions expressed in this report reflect only the views of the authors and in no way bind CERRE, the sponsors or any other members of CERRE (www.cerre.eu).

About the authors

Pierre Larouche is Professor of Competition Law at Tilburg University and Founding Director of the Tilburg Law and Economics Center (TILEC), as well as Professor at the College of Europe (Bruges) and Joint Academic Director of the Centre on Regulation in Europe (CERRE). A graduate of McGill, Bonn and Maastricht, he clerked at the Supreme Court of Canada in 1991-1992 and practised law for three years before joining academia. His teaching and research interests include competition law and economic regulation, electronic communications law, media law, comparative law and tort law. He has been a guest professor or scholar at McGill University (2002), National University of Singapore (2004, 2006, 2008, 2011, 2013), Northwestern University (2009-2010), Sciences Po (2012) and the University of Pennsylvania (2015).

Martin Peitz is a Joint Academic Director of CERRE and Professor of Economics at the University of Mannheim. He is also Co-Director of the Mannheim Centre for Competition and Innovation (MaCCI). Martin is a member of the Economic Advisory Group on Competition Policy (EAGCP) at the European Commission. He is Co-Editor of 'International Journal of Industrial Organization', Associate Editor of 'Journal of Industrial Economics' and 'Information Economics and Policy', and member of the editorial boards of 'Telecommunications Policy' and 'Journal of Media Economics'. He is a research fellow of CEPR, CESifo and ENCORE, and a research associate at ZEW. He has published widely in leading economics journals and is the author of the books 'Industrial Organization: Markets and Strategies' (with Paul Belleflamme) and 'Regulation and Entry into Telecommunications Markets' (with Paul de Bijl), both published by Cambridge University Press. His research focuses on industrial organisation, regulation, and microeconomics.

Nadezhda (Nadya) Purtova is Assistant Professor at Tilburg Institute for Law, Technology and Society. Her research interests include comparative data protection and information privacy law and property law, as well as economics of data protection law. She was awarded the Tilburg Best Doctoral Dissertation Award for her doctoral dissertation 'Property rights in personal data: a European perspective', which is published by Kluwer Law International. In recent years Nadya was also involved in research on the privacy and safety aspects of eHealth, privacy of health data, and the economic analysis of data protection law. She holds an LLM from Central European University, an MSc from Leiden University and received her PhD *cum laude* from Tilburg University.

Executive Summary

Privacy and data protection have become crucial issues in network industries. With the increasing amounts of data collected (e.g. Internet of Things) and with advances in processing (e.g. Big Data), data now plays a central role in firms' strategies. This affects all network industries, not just the communications and information cluster. Much of the data collected is personal data, i.e. data relating to an identified or identifiable natural person, hence the creation of privacy and personal data laws in the US and the EU.

Consistent, future-proof regulation requires a common approach to all industries, regulated and unregulated alike. Sector-specific privacy regulations are inadequate in a dynamic environment and should therefore be withdrawn.

From an economics perspective, privacy and the protection of personal data can be seen as services over which parties may transact: these parties include individuals holding personal data, firms wanting to use that data, information intermediaries dealing in personal data, public authorities and privacy providers. As shown with the example of targeted advertising - one of the most common applications of personal data – the disclosure of personal data is neither categorically good nor bad for consumers and society. A simple property rights analysis cannot suffice to evaluate welfare effects of the disclosure of personal data. Classic market failures around information disclosure could prompt, but do not unambiguously justify, public intervention. The set of environments under which consumers benefit from restrictions imposed on the commercial collection and use of personal data is, however, limited. In many environments, firms and consumers actually gain from disclosure, creating a win-win situation. A more important concern is the extent to which consumers are able to properly evaluate the costs and benefits of disclosing personal data. Empirical research points to a 'privacy paradox', a discrepancy between the stated preference for privacy protection and the observed behaviour of customers. This provides a strong justification for mandatory minimum requirements on privacy protection.

As regards law and regulation, a European approach has emerged, based on the fundamental rights to privacy and to personal data protection, and enshrined in the EU Data Protection Directive and the proposed General Data Protection Regulation. The EU approach, in its generality and broadness, contrasts with the US approach, which is much more piecemeal and puts more emphasis on freedom of expression and of commerce than on privacy and personal data protection. The core of EU data protection law lies in the principles of data processing on lawful grounds only, for legitimate purposes; transparency; minimisation of personal data processing and storage; accuracy of personal data; security of personal data; effectiveness of data protection and accountability of data controllers. Data subjects hold a number of rights, including the right to information, to access personal data, to rectify it, to object to processing and to erase personal data ('right to be forgotten').

EU privacy and data protection law, however, suffers from a 'reality gap', or disconnect. In substance, it is not entirely adapted to data-centric business models (including Big Data), as opposed to business models where data processing is ancillary to a main business. In addition, when it comes to enforcement, the public enforcement model cannot cope, because national Data Protection Authorities lack resources and jurisdiction is not always clearly established.

Such a disconnect is no reason to abandon the EU approach, in favour of self-regulation in the US style. Rather, we recommend that EU law be cast as a baseline, as a guide to private parties in their dealings on and around privacy. Using that baseline, private activities can then be given a greater role in the enforcement and development of privacy and data protection in the EU. Private enforcement – via liability – can supplement public enforcement, and private incentives to offer contractual protection over and above the baseline can be encouraged.

Unfortunately, the legislative procedure on the proposed GDPR[1] threatens to unravel the baseline function of EU law. Instead of trying to provide for every possible exception, special case, etc., and to reserve room for Member State to enact their own legislation, the EU institutions should focus the GDPR on the main principles, and accept that issues will arise later in the life of the GDPR, that will require interpretation and further elaboration.

The EU Data Protection Directive leaves room for private parties to influence personal data protection, via codes of conduct, to which the General Data Protection Regulation would add certification and trust seals. These instruments are primarily conceived from a public law perspective, i.e. as private mechanisms complementing public enforcement.

We strongly recommend that, in the finalisation and implementation of the General Data Protection Regulation, more room be given to private law mechanisms. When data controllers fail to meet the baseline of protection, private enforcement (via liability) could add muscle to the law and contribute to reducing the reality gap. For that purpose, the liability regime should be more fleshed out, including the basis for liability and defences, as well as the use of collective redress mechanisms. When data controllers want to go beyond the baseline of protection, a properly functioning market is needed. This is where a strong data portability principle, coupled with competition law enforcement, can play a role.

Public authorities should also play a more proactive and advocacy role in ensuring the success of codes of conduct, certification and trust marks, in order to mitigate well-known market failures related to information or decisions that are not widely observable, once firms start to offer superior privacy and personal data protection.

[1] In December 2015, as this project was concluded, the EU institutions agreed on a compromise text for the General Data Protection Regulation. The compromise text does not differ from the negotiating texts available at the time of writing, and therefore does not affect the analysis conducted in this report. However, a number of relevant points are discussed in the Postscript.

1. Introduction

At a time when discussions on a new EU General Data Protection Regulation (GDPR) are reaching their final stage, and implementation and compliance starts to draw attention, this report advocates a 'mainstreaming' of EU data protection laws, i.e. a greater effort to insert these laws in the broader legal and economic context of business transactions, and, next to the public law approach to data protection as a fundamental right, also profit more from advantages that private law mechanisms offer, notably, to the enforcement framework.

This argument is distinct from the mainstream view of what constitutes a market approach to privacy and data protection. In the context of the debate about property in personal data, it is often argued that privacy is a *public good* and that the market is unable to provide for it. For instance, Byford submits that regarding 'privacy as an item of trade … values privacy only to the extent it is considered to be of personal worth by the individual who claims it'.[2] Pamela Samuelson argues that propertisation of information privacy as a civil liberty might be considered *morally obnoxious*.[3] 'If information privacy is a civil liberty, it may make no more sense to propertise personal data than to commodify voting rights.'[4] However, what this report argues is not that data protection should be left to market forces. Rather, we submit that in the circumstances when the amount of information processed globally is estimated in zettabytes (1.2 zettabytes, or 1,200,000,000,000,000,000,000 bytes) and growing at a rate of 60% per year,[5] public enforcement mechanisms could use the help of market forces in upholding public law principles regarding how this data is processed. Our argument does not touch on the substantive principles of data protection, both because they constitute the baseline of protection which, we claim, should not be subject to market negotiation, but also because the adequacy of the current substantive principles of data protection, such as the principle of individual control, in the current realities of ubiquitous and omnipresent data collection and processing is increasingly questioned.[6]

The report first surveys the significance of consumer privacy in network industries, in the light of technological and economic developments, and introduces privacy and data protection legislation (Section 2).

In the next part, the report provides an economic analysis of privacy, grounded in academic economic literature, with a view to introducing the reader, in a structured way, to the main insights coming out of the work of economists on privacy (Section 3). That work contains theoretical and empirical investigations, emphasising perspectives from information and behavioural economics. In line with the general analytical approach of economics, privacy and

[2] K.S. Byford 'Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment' (1998) 24 Rutgers Computer & Tech LJ 1.
[3] P. Samuelson 'Privacy as Intellectual Property?' (2000) 52 Stanford L Rev 1125 at 1143.
[4] *Ibid*.
[5] The Economist, 'Data, Data Everywhere' (27 February 2010) 1.
[6] E.g. B.-J. Koops 'The trouble with European data protection law' (2014) 4 International Data Privacy Law 250.

private information are seen from a transactional perspective, as information goods that can be part of transactions and therefore have an impact on individual and social welfare. That impact is neither unreservedly good nor bad, however, and accordingly a cautious approach to privacy regulation is warranted.

Against that background, Section 4 then sketches the main lines of EU privacy and data protection regulation, contrasted against corresponding US law. EU regulation takes a more prescriptive route than the economic analysis would suggest, since it starts out from a fundamental rights rather than a transactional perspective.

Section 5 contains the more detailed analysis of why and how EU privacy and data protection regulation should make more room for private law, both in substance and as regards enforcement.

2. Significance of consumer privacy issues in network industries

Privacy and data protection issues have been with us for decades, but they have become increasingly salient lately, due to the convergence of a number of factors.

First of all, the amount of data generated and collected has grown massively. Whereas in the past data was often manually generated by users (data subjects) and painstakingly collected by firms, now digitalisation and the omnipresence of sensors allows for the production of data on an unprecedented scale, whether it concerns transactions, communications, preferences, opinions, relationships, location, movement, activity, health or ambient conditions, among others.

This development reaches its next phase with the Internet of Things (IoT), where objects – household appliances, cars, consumer goods, etc. – are also able to generate observational or status data, and communicate that data directly to other objects. In parallel, the cost of data storage continues to decrease, so that it becomes practicable to store a significant amount of the data generated.

With the increased generation and storage capacities, comes also the increased ability to analyse collected data, often referred to as 'Big Data'. As described in a leading monograph,[7] Big Data involves (i) the ability to analyse the entire data, as opposed to just a sample, coupled with (ii) a relaxation in requirements as to the exactness of the data and (iii) a shift from external to internal validity. As data are collected from a large fraction or even the full consumer population, the representativeness of the sample is no longer an issue. Big Data enables firms to derive valuable information – and often fundamental insights – that lead to new and improved offerings to customers.

From a business perspective, these developments propel data from an ancillary to a central role. Whereas a generation ago, a firm managed data as a back-office function – to keep a record of its customers, suppliers, etc. – to support its primary processes, data is now part of these primary processes. It is used to drive strategy, product development, advertising and marketing, sales, and every other firm function. What is more, for many firms, data *is* the primary process: they are engaged in data collection, processing and analysis as their main activity.

Network industries are affected by these developments just like other consumer goods or services industries in which a lot of personal data can be collected. Of course, this applies to the ICT cluster. Even then, while computer and information technology firms were always dealing with data, telecommunications firms used to collect limited data about the use of their networks (essentially call data). As they are morphing into broadband access providers, electronic communications firms – fixed and mobile alike – are collecting and generating masses of data

[7] V. Mayer-Schönberger and K. Cukier, *Big Data* (London: John Murray, 2013).

about their users: download and upload volumes, IP addresses, traffic patterns, etc. At the request of law enforcement and intellectual property owners, electronic communications firms are also required to increase their ability to collect further data from their users.

In the energy sector, the deployment of smart meters is changing the position of energy providers. Whereas previously data was collected very sporadically (meter readings approximately once a year) for the backoffice, now smart meters return real-time usage data that can be used to improve the quality of service to users, but also for other purposes such as energy policy (consumption management), security, etc.[8]

Industry example 1 (smart metering)

In contrast to traditional meters, smart meters automate reading and provide high-frequency consumption data. In electricity, time-dependent prices (mostly together with 'smart' household appliances) may allow for consumption smoothing and may thus reduce the need to install additional generating capacity. Smart metering raises privacy and data security issues when personal data are involved. Any data that are linked to an individual identifier – in the case of smart metering this is the meter number and any information on an individual including electricity consumption – constitute personal data.

Regarding data protection legislation at the European level, not only the Data Protection Directive, but also the e-Privacy Directive[9] are applicable to smart metering. Firms collecting and processing personal data are considered to be data controllers who are then obliged to comply with data protection legislation. Data controllers must make sure that consumers have access to their personal data and that they give consent to data processing. While typically several actors are involved in the processing of data, it may be best for the functioning of the market to have a single firm in the system serving as the point of contact for consumers.

While the current view of the role of data from smart meters is that it allows for a more efficient functioning of the utilities involved, these data (as personal data or at a more aggregate level) are potentially also useful for third parties offering products or services to consumers, as they can reveal a lot of information on consumer habits and tastes, which are otherwise difficult to obtain.

Similarly, in the postal sector, the introduction of tracking systems allows postal operators to provide more elaborate services and integrate their operations better with those of their clients. By the same token, troves of data about mail and package flows are generated.

In the rail transport sector as well, the widespread use of digital tools for the issuance and control of tickets, combined with digital real-time timetables, allow operators to provide more elaborate services to travellers (before and during their travel), and to collect data on travel and travel preferences.

[8] CERRE, *Regulating Smart Metering in Europe: Technological, Economic and Legal Challenges* (31 March 2014), available at www.cerre.eu.
[9] Directive 2002/58 of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive) [2002] OJ L 201/37.

Industry example 2 (passenger rail)

With the prevalence of electronic ticketing and a widespread use of loyalty programmes in passenger rail,[10] rail companies can collect data on consumer mobility. This information is potentially useful for capacity management and the application of yield management techniques. It becomes particularly relevant when a large fraction of consumers use a loyalty card for passenger rail services.

Detailed consumer data also enable rail services providers to target ancillary products offered by third parties on their website or mobile app, such as rental cars, hotel rooms, insurance, and restaurant discounts or vouchers.[11] The associated privacy issues are similar to those arising with loyalty cards issued by airlines and retailers.

With mobile apps (possibly using geo-tracking), additional services such as information on connecting trains and local transport can be provided which lead to a better consumer experience. Overall, providers of passenger rail services may become providers of general mobility and travel services targeted to consumer needs and tastes. Some of them will be provided in-house, others by selected partners, and yet others on an open market place.[12]

For all firms interacting with consumers, in the network industries and elsewhere, data becomes an input for a range of services to be offered now or in the short term. In addition, data has strategic value, as a source of information for the development of new offerings, whether in-house or in collaboration with partners.

Of course, most of the data collected and generated concerns users of the services offered by these firms. The data constitutes information about the characteristics, tastes and preferences of individual users. In legal terms, it is 'personal data', i.e. information relating to an identified or identifiable natural person.[13] Typically, individuals are concerned – to a varying extent – about the collection and processing of personal data by outside parties, for a number of reasons. Many of these reasons are elaborated upon later in this report. They include: (i) a perception that personal data is private to the individual, so that its collection and processing represents an intrusion into the private sphere, (ii) a fear that such personal data might be misused or abused[14] to the detriment of the individual (that detriment can be economic or social), (iii)

[10] In the example of Deutsche Bahn, this is the bahn.bonus programme which works similar to a frequent flyer card issued by an airline.
[11] The website or mobile app then becomes a platform. While operating such a platform does not require detailed consumer profiles, offerings can be targeted more effectively when such data are collected and used.
[12] Alternatively, third-party platforms may include rail tickets as part of their product portfolio on offer.
[13] Directive 95/46 of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 [hereinafter DPD], Art. 2(a). That person is then called the 'data subject'. Art. 2(a) goes on to specify that 'a identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'. The proposed General Data Protection Regulation [reference in Annex, hereinafter GDPR] retains the same definition at Art. 4, adding however a longer list of factors that can make an individual identifiable.
[14] The misuse or abuse can be either intentional by the outside party, or arise as a result of a negligent use of personal data, which would lead to a security breach and a leak to unauthorised parties.

commercial use of data which ultimately may not be in the interest of the consumer providing those data or of the consumer population at large.[15]

These concerns have prompted public authorities to enact laws and regulations concerning the protection of privacy and of personal data. The core of these laws and regulations, in the EU and in the US, is set out further in Section 4. In recent times, privacy and data protection laws have gained increased visibility, following a number of high-profile incidents and cases that resonated worldwide.

The need for legal protection, as well as the ease with which it can be circumvented, was driven home in the Snowden case, which revealed large-scale eavesdropping by the NSA, outside of legal control. For the purposes of this report, however, we focus on privacy and data protection in relation to the actions of private firms, and will leave aside protection in relation to the actions of public authorities.

A constant stream of well-publicised security breaches, where the personal data of consumers is compromised and exposed to often malevolent third parties, also contributes to the unease of the general public and feeds calls for legal intervention or better enforcement of existing laws.[16]

Two recent ECJ cases show that the law is not entirely powerless. In *Google Spain*,[17] a Spanish national, Costeja González, complained to the Spanish data protection authority, in order to force Google to modify its search algorithm. When Mr. González's name was queried on Google, Google returned a link to decade-old newspaper articles concerning a forced sale of Mr. González's assets in order to recover social security debts. Considering that that proceeding had been resolved, Mr. González invoked the 'right to be forgotten'. The ECJ found that Google was subject to EU data protection law and that it had to comply with Mr. González's request, since his right to privacy and to the protection of personal data, in the circumstances of the case, overrode Google's commercial interest and the interest of other users in having access to the articles in question. The *Google Spain* judgment was generally welcomed in Europe, but almost unanimously disapproved of in the US. Nevertheless, Google chose to comply with the judgment and took measures to implement a 'right to be forgotten', at least for EU-based individuals.

Very recently, in *Schrems*,[18] the ECJ invalidated the Commission's decision approving the 'safe harbour' agreement with the US, for the purposes of the application of the DPD. Under that agreement, the US had introduced a legal framework (albeit not legislative) for US firms to commit to provide an 'adequate level' of personal data protection within the meaning of the DPD.[19] With its decision endorsing the US framework, the Commission had provided a general

[15] Section 3 of this report is dedicated to the analysis of the economic effects of the commercial use of personal data.
[16] See the Privacy Rights Clearinghouse, at www.privacyrights.org, a non-profit that maintains a list of breaches involving US firms. A staggering 4600 breaches are listed since 2005, for a total of close to 900 million breached records.
[17] Case C-313/12, *Google Spain* v. *AEPD*, ECLI:EU:C:2014:317 (13 May 2014).
[18] Case C-362/14, *Schrems* v. *Data Protection Commissioner*, ECLI:EU:C:2015:650 (6 October 2015).
[19] Art. 25 DPD.

authorisation for personal data transfers between the EU and US.[20] The ECJ held that the Commission could not validly approve the 'safe harbour' approach of the US, since the US had reserved the ability to let US law on national security, public interest or law enforcement prevail over personal data protection, without sufficient safeguards. Here as well, the judgment of the ECJ threw a spanner in the works of EU-US relations as regards privacy and data protection. It remains to be seen how the Commission and its US counterparts will respond to the ECJ ruling.

While these two ECJ cases provide a good illustration of the reach of EU legislation on privacy and data protection, they also lay bare the differences between the US and the EU, which will be explained in greater detail in Section 4. As was mentioned above, one of the most significant business developments in recent years was the rise of data-centric business models, where data collection, storage and processing is at the core of the activities of the firm. These data-centric firms emerged in the US to become global giants. While they are essentially US-based, they offer their services in the EU as well. Their own approach to privacy and personal data ('privacy policy') is largely influenced by US law, which is less prescriptive, as will be seen below. Accordingly, for many of these firms, it proves difficult to come to grips with the privacy and data protection laws in Europe, which do not match – or even contradict – their own privacy policy. Since data is at the core of the business of these firms, the application of the privacy and data protection laws of Europe therefore has a direct effect on their business prospects, hence the sensitivity of the issue.

Given the distance between the 'home-grown' privacy policies of many data-centric firms and privacy and data protection laws of Europe, compliance is key to the effectiveness of the laws of Europe. On that point, despite high-profile ECJ judgments such as *Google Spain* or *Schrems*, there is still a perception that privacy and data protection laws in Europe suffer from a 'reality gap': compliance is not as thorough as the official discourse would make one believe.

When it comes to network industries, general data legislation in the EU may be complemented by sector-specific privacy regulation. This is problematic for at least two reasons. First, regulation may be inconsistent and create legal uncertainty due to conflicting provisions in sector-specific and general privacy regulation. Whenever this occurs, it is an instance of bad regulation which can be remedied by harmonising sector-specific and general regulation. Such harmonised regulations could live happily side by side, as long as there is a clear and stable link between specific privacy concerns and the particular sector to which the sector-specific regulation applies.

The previous observation leads to the second and more fundamental problem. Sector-specific regulation has to take a stance on which firms and activities to include, which almost invariably leads to boundary problems in the application of the law. However, the need for different levels of privacy protection arises because some types of personal data are more sensitive than others. It does not arise because of the particular type of service generating those data. In a dynamic

[20] Other means of authorising personal data transfers to third countries are available at Art. 26 DPD, including a list of legitimate purposes (consent of the data subject, contractual performance, important public interest grounds) or the provision of sufficient contractual safeguards (including Binding Corporate Rules, discussed further below).

environment with frequent introductions of new services, any regulation based on the type of service rapidly becomes outdated. Apart from failing to provide adequate protection, another downside of such regulation is a likely distortion of competition. A case in point is the e-Privacy Directive,[21] which does not make all services involving similar types of personal data subject to the same regulation and treats telecommunications providers and some so-called "over-the-top" players differently even though they transmit similar type of data.

Industry example 3 (traffic data)

Traffic data is the data that is processed in the course of making a communication on an electronic communications network, i.e. the number of a person called, or the address on a packet of data to be conveyed on an IP network.[22] That data can be processed to provide various services to the user, beyond the communication itself, such as preferential rates based on frequently-used numbers or data traffic volume or destination. Pursuant to the ePrivacy Directive, electronic communications providers must obtain the consent of the data subject before using traffic data to provide any service going beyond the communication itself.[23] The ePrivacy Directive does not allow any other ground for personal data processing than consent. In comparison, service providers falling outside of the definition of electronic communications networks and services (such as most so-called Over-The-Top or OTT providers) are subject to the DPD only, pursuant to which processing of personal data can be done on other grounds besides consent.[24] Despite the fact that some of their respective services are in direct competition with one another (voice and VoIP, SMS and text messaging, cable and IPTV), electronic communications providers and OTT providers are subject to differing personal data regulation.

A future-proof privacy regulation would instead define general principles, possibly with special provisions for particular types of personal data (e.g. personal information on health and financial status) that apply across all sectors of the economy (including, but not being restricted to, network industries). As a consequence, sector-specific privacy regulation, in particular the ePrivacy Directive, would need to be closely examined to ascertain whether it provides any added-value over and above the DPD (and soon the GDPR). In the course of doing so, the following parameters should be taken into account: (i) a counterfactual: what would happen without the ePrivacy Directive, i.e. what would be the outcome if only the DPD (or GDPR) were applicable?; (ii) a comparison: what does the ePrivacy Directive add in the light of the counterfactual?; (iii) a characterisation: if there is any added value, is it a matter of substantive law or rather a matter of additional enforcement resources? In the latter case, this does not justify a specific directive; (iv) trade-offs: if there is any added value, are there any associated disadvantages, such as a distortion of competition (between firms subject to the Directive and those outside of its scope) or an impact on innovation. At the end of this process, the ePrivacy

[21] *Supra*, note 8.
[22] That address is a set of four hexadecimal numbers that can convert into an e-mail address, a URL or another form of address, depending on the application used.
[23] This requirement flows through the whole ePrivacy Directive for all data collected by electronic communications providers; in the case of traffic data, see in particular Art. 6(2) and Rec. 30.
[24] See DPD, Article 7, explained below under Heading 4.

Directive should be shortened accordingly, or withdrawn altogether (some of its elements might also be extended to all firms and picked up in the GDPR[25]). Since the proposed GDPR is not intended to supersede sector-specific regulation, there appears to be a missed chance to streamline privacy legislation at the European level.

[25] For instance, the provision on cookies, at Art. 5(3) of the ePrivacy Directive, applies to all firms, and on that account could be picked up in the GDPR.

3. Economics of privacy

From an economic perspective privacy can be treated as a service, which may be included in a transaction or relationship. Economics provides tools to analyse the impact of market behaviour on consumer privacy; it does not take a stand on the value of privacy. In most cases the presumption is that privacy enters into a consumer's utility or well-being, where it is up to the individual consumer to decide which kind of information disclosure (potentially limited in the audience) affects a consumer's benefit positively or negatively. Economic analysis has highlighted mechanisms that uncover potential tensions between firms' incentives on the one hand, and consumer interests and society's benefits on the other. It also identifies circumstances under which firm and consumer interests are aligned.

This section presents a framework to think about privacy by identifying the relevant parties. It discusses in general terms the potential gains and losses of privacy before presenting some of the economic mechanisms at work, in particular, as they regard the monetisation of personal data and its impact on consumer and societal welfare.

3.1. Privacy policy and affected parties

Privacy policies affect the benefits different parties obtain from market transactions.[26] Privacy infringements, or the possession and (mis)use of personal data, may also directly affect the well-being of individuals. Economists have been focused on measuring and understanding the first type of effects; however, there is also some work that is helpful to address the second type of effects.[27] A simple short-cut to incorporate the second type of effects is to consider perceived privacy infringements (no matter whether they are legal) as imposing a cost (or loss of well-being) on the person suffering the infringement irrespective of the economic consequences of this infringement.[28]

It is useful to categorise the parties involved in privacy issues. First, there are *individuals* who hold personal information. Second, there are *firms* (producers and retailers) who may want to

[26] There are a number of excellent surveys on the economics of privacy. These include K. Hui and I. Png 'The economics of privacy', in T. Hendershott, ed., *Handbooks in information systems: Economics and information systems* (Amsterdam, Elsevier, 2006), L. Brandimarte and A. Acquisti 'The economics of privacy', in M. Peitz and J. Waldfogel, eds., *The Oxford handbook of the digital economy* (Oxford: Oxford University Press, 2012), C. Tucker, 'Social networks, personalized advertising, and privacy controls' (2015) 51 Journal of Marketing Research 546 and, in particular, A. Acquisti, C.R. Taylor and L. Wagman 'The economics of privacy' (2015) forthcoming in Journal of Economic Literature. We refer to these works for an extended discussion of the economics literature on privacy; in this section, we aim at highlighting a few mechanisms that we deem to be relevant to be kept in mind in the policy debate.

[27] As pointed out by J. Farrell, 'Can privacy be just another good' (2012) 10 Journal on Telecommunications & High Technology Law 251, the former corresponds to privacy as an intermediate good, while the latter corresponds to privacy as a final good. In the public debate, privacy as a final good appears to be of particular importance and we take note that economic theory has little to say on this if privacy is treated as a fundamental right, as this makes it difficult to engage in a discussion of (economics) trade-offs. However, a fundamental rights perspective can be included in the economic analysis by defining constraints imposed by society. Such constraint defines which type of information can be disclosed, by whom, to which parties, and for which period of time.

[28] This second type of effects comes closer to the fundamental rights approach informing EU law on the matter.

use this information to improve their selling mechanisms (e.g. through behavioural targeting of ads, price discrimination) or their overall performance (e.g. management of warehouses, introduction of new products). Third, there are *information intermediaries*, who may collect information on individuals, aggregate this information, and sell it to firms or use it in the interest of firms (e.g. by allowing targeting of ads).[29] These information intermediaries include Internet giants such as Amazon, Apple, Facebook, Google, and Microsoft. Such intermediaries do not necessarily collect data themselves; they also aggregate data from sellers, intermediaries and publicly posted information.[30] Firms rely on information intermediaries or collect data themselves (as is typically done by firms issuing consumer loyalty cards). Personal information may be used for advertising in sponsored search (Google or Bing by Microsoft), targeted display advertising in social networks (Facebook), or product recommendations in curated retail environments (e.g. Amazon or Apple iTunes). And fourth, the *government* (including possibly independent regulators and competition authorities) may be an actor that regulates privacy or applies general competition law to cases with a privacy dimension. Fifth, to the extent that individuals seek privacy protection beyond what is imposed by the government, *privacy protection services* may be viable on a commercial basis. Providers of such services would then contract with individuals, and possibly also with firms to commit to certain privacy and data protection standards.

We would like to point out that the actions of each of these five groups of actors impact the availability and use of personal data. Clearly, the individual can take actions that limit the disclosure of personal information.[31] All other actors can formulate a 'privacy policy' setting out their approach. Sellers may communicate their privacy policy to individuals. They may tell individuals for which limited purposes they collect certain information (e.g. collect addresses only for shipping purposes). Similarly, information intermediaries may commit to a privacy policy, e.g. committing to not revealing personal data to sellers and only using their data to offer segmented advertising possibilities. Last but not least the government may want to intervene, rule out the collection of certain types of data, impose opt-out or opt-in rules, or impose requirements that data can only be kept for a limited period of time.[32]

[29] As mentioned above, current EU data protection law might not adequately account for the type of data-centric business models pursued by these intermediaries.

[30] Alice E. Marwick ("How Your Data Are Being Deeply Mined", in New York Review of Books, January 9, 2014) reports about Acxiom, the second largest American firm providing database marketing. This firm keeps records of hundreds of millions of US citizens and residents. It has an average of 1500 pieces of information on each individual which includes information from publicly available records (home valuation, vehicle ownership), information about online behaviour (tracked through cookies, browser advertising), and data from customer surveys and "offline" buying behaviour. On its website Acxiom announces that "[it] connects people across channels, time and name change at scale by linking our vast repository of offline date to the online environment" [http://www.acxiom.com/data-packages/, last accessed September 5, 2015].

[31] Part of the academic and policy discussion on privacy is to what extent the individual really is able to exert control over his or her personal data. We address this issue further below.

[32] We deliberately do not include the government as an entity that legally (or illegally) collects personal data for its own purposes (e.g. to combat tax fraud, uncover harmful behaviour by individuals, or punish individuals who question certain government actions). Here, the government is a regulator of itself (or, more precisely, of government

Privacy policies may involve different types of commitments:

- A party may commit not to collect or not to store certain types of information or only for a limited amount of time.
- A party may commit to use certain types of personal information only for limited purposes.
- A party may commit not to combine the personal data it obtained from individuals with other data sources (which may be publicly available – e.g. public Facebook profiles – or through other 'private' channels, such as other services it offers or the acquisition of third parties)
- A party may commit to pass on information only in anonymised form (which does not allow for matching with other data) or, even, not to pass it on at all.
- A privacy policy may also contain the possibility for individuals to keep track of all the personal data available to the collecting party and may involve the option to (selectively) remove personal data.

3.2. Gains and losses from privacy

Firms (in particular, advertisers) and information intermediaries may want to engage in targeting, which so far appears to be the main use of increased collection, storage and analytical abilities with respect to personal data. The current data gathering activities and efforts by information intermediaries to provide highly segmented audiences suggest that at least information intermediaries must think that this is a valuable service which allows them to obtain additional profits. For the individual advertiser, targeting based on individual characteristics or behaviour may be attractive for a number of reasons:

- The advertising budget can be targeted towards core customer groups.
- Targeted advertising allows the firm to experiment with different sales strategies to learn about how consumers react (here, consumers of the same or similar type see different ads).
- The advertising message can be fine-tuned.
- A highly segmented demand side allows a firm to test waters (e.g. by geographic targeting).
- Targeted advertising may make it attractive to offer a diversified product portfolio to cater to a variety of different tastes; this may allow the firm to obtain larger revenues.
- Targeted advertising (in particular, in social networks) may allow more effective product introductions (advertising targeted at people with particular network characteristics). This in turn might lower barriers to entry, especially for smaller firms.

agencies). We admit that the use of personal data by governments may constitute the most severe privacy violations. However, they are outside the focus of this report, as they do not constitute a commercial use of personal data.

- Targeted advertising may allow a firm to better engage with different customer groups and thus increase the attachment of those customers (e.g. video clips with group-specific celebrities)
- Beyond targeting, personal data may help firms in their strategy to successfully introduce differentiated products. It may, in particular, help firms in steering their efforts towards quality improvements that are sought after by consumers.

However, there are also a number of possible downsides of targeting, for instance:

- Targeted advertising, when offered by information intermediaries, may come at a higher price than less-targeted advertising.
- If the data collection is done in-house, the firm incurs higher costs in implementing its advertising strategy.
- Privacy concerns by consumers can lead to a backlash; in extreme situations, the reputation of a firm is at risk.
- In case of security breaches, holding personal data may lead to costs for the firm (monetary or through a loss of trust and reputation).

Since some consumers are more sensitive to disclosing personal information than others, firms and information intermediaries may engage in offering consumers a menu of privacy options. Also, there are different market places which also differ in the required disclosure of personal information. Consumers, therefore, have to make a choice whether, and to what extent, they are willing to disclose certain information in a specific market environment.

Disclosing personal information has a number of potential benefits for an individual consumer. Direct benefits in consumer-advertiser relationships include the following:

- The consumer receives 'better' product recommendations; i.e. there is a better match between product characteristics and consumer preferences (which may be context-dependent). A particular instance of advertising responding to context-dependent consumer preferences is geo-targeting: a consumer at a particular location may receive ads from shops located nearby.
- Alternatively, the consumer has fewer searches to do and, thus, incurs lower search costs.
- The consumer receives particular personalised offers or suggestions for personalisation (as an extreme example, targeted advertising may be combined with 3D-Printing).
- Since a consumer is not interested in a number of products or product categories, targeted advertising can reduce the amount of 'spam' advertising; this may lead to a decrease of overall ad exposure or provide firms with niche products with the possibility to address potential customers.
- Revealing personal information may not be undertaken with the consumer-advertiser relationship in mind, but for other purposes.

- If the information intermediary is a social network, disclosing information improves communication with other network members and may also give rise to new links in a network.
- If the information intermediary provides 'free' content, disclosing information allows for a better match between 'free' content and the individual's preferences for content (e.g. the outcome of an organic search query could depend on the – possibly context-dependent – characteristics of a consumer).
- An individual may disclose personal information to improve his or her status within a community or give rise to non-monetary rewards. The latter is the case, if a consumer (e.g. on a platform such as TripAdvisor) obtains a badge by providing feedback.

Disclosing personal information, however, may come at a cost to consumers:

- If an information intermediary has access to personal data it can provide advertising to specific audiences, which may make it attractive for advertisers, who otherwise would not be active, to address these consumers. Thus, ad levels may actually go up (above we mentioned the opposite possibility, namely that it goes down).
- If firms correctly target their ads, they know that they reach consumers with a higher willingness to pay. This may induce them to increase the price.[33]
- Consumers may suffer from the accidental disclosure of information and the resulting actions by firms.
- Consumers may suffer from the unforeseen use of personal data (including reputational effects).
- Consumers may suffer from the unforeseen combination with other publicly available data or data from other sources, and the use of the resulting expanded data set by firms.
- Consumers may suffer from a misuse of personal data by the party to which this information has been disclosed or from criminal behaviour by third parties (who gain access due to security problems).
- Consumers may suffer a psychological discomfort from the mere fact that some personal information is in the hands of some other party (a particular advertiser or an information intermediary).

A first general insight is that the release of personal data by individuals is neither categorically good nor categorically bad for society. Also, from an individual's perspective, there are situations in which the disclosure of certain personal information to a particular group of addressees is desirable and there are other situations, other elements of personal information and other groups, where it is not. Claims that more release of personal information is categorically good or categorically bad (from the point of view of the individual or of society) can

[33] This is not necessarily the case. Targeting may increase the competition among firms with the effect that prices may actually fall. We look at this issue in more detail further below.

easily be shown to be wrong. Thus, we will have to take a closer look at the mechanisms at play when the release of personal information is an issue. Clearly, the individual and society may form different opinions on the desirability of certain market outcomes and possible regulatory interventions.

From a social perspective, when concerned with overall well-being, the analysis tends to focus on inefficiencies, whereas the individual is concerned with personal well-being, which includes redistributive effects of policy changes. This does not mean that society does not care about the distribution, but that this often exists as a second thought.

Since privacy, to a large extent, concerns the disclosure and use of information and associated trade-offs, both from an individual and a societal perspective, economics provides useful tools and methodologies for analysing its effects.

3.3. A simple property rights analysis

As a starting point, we will follow a property rights approach. The deliberate disclosure of personal information is then seen as an act by one party within a contractual relationship with another party.[34] Under some idealised circumstances, an individual initially holding the property rights over his or her personal data, should only engage in transferring some of these rights if this is in his or her interest.

One way by which privacy regulation affects market activities is in restricting the disclosure of information.[35] From the viewpoint of the firm possibly acquiring personal data, this means that privacy regulation restricts the collection of information.[36] It is useful to start by considering a fictional individual who assesses the private costs of disclosing personal data correctly. In such a case, one may think that information disclosure in unproblematic, since parties agree on such a transaction, and the individual would only approve it if this is in her interest (e.g. because she obtains a monetary or in-kind payment, or because she receives better subsequent offers). This would suggest that privacy regulation is necessarily harmful, as it may destroy contracting among parties that would realise positive gains from trade.

Indeed as has been argued,[37] privacy protection imposed by a regulator leads to inefficiencies as it precludes certain contracts that are to the benefit of both contracting parties. Privacy regulation thus stands in contrast to unlimited freedom of contract, and it may impose a cost on the parties which would have contracted, absent this regulation. Gains from trade may not materialise; in addition, there may be redistributive effects as parties with, from the viewpoint of the counter-party, unfavourable private information may become indistinguishable from

[34] On the definition of personal data in the context of DPD see Heading 5 below.
[35] It may also restrict the use of data by the party gaining access to them. For instance, it may require the party to remove those data after a certain period of time, not to share these data with other parties, or not to use the data for certain purposes itself.
[36] Privacy regulation may alternatively limit the use of information. For instance, firms may be allowed to track individual behaviour, but they may be prohibited from making discriminatory offers based on this information.
[37] See R.A. Posner, 'The economics of privacy' (1981) 71 American Economic Review (Papers and Proceedings) 405.

parties with favourable information (see e.g. Stigler, 1980). These redistributive effects may be socially desirable or undesirable.

However, the view that an individual engages in disclosing personal information only if this is in his or her interest, so that privacy regulation would be harmful, can be challenged on a classic market failure analysis (sections 3.4.1 and 3.4.2 below), as well as on the basis of 'biased' decision making by the individual (section 3.4.3. below).

Once asymmetric information is factored in, effects on welfare and the surplus of individuals are, in general, ambiguous. Privacy regulation that prohibits the disclosure of information may then actually increase social welfare. One reason is that, absent regulation, the counter-party may overinvest in collecting information, as private benefits may at least partly stem from a redistribution of rents. This does not increase social welfare and, therefore, does not affect the social benefit from collecting information.[38]

In response to that, one may think that by assigning property rights (e.g. the right of an individual to conceal information) market outcomes can be affected to the benefit of the individual and society at large. Put more strongly, one may think that inefficiencies as a result of asymmetric information problems can be successfully remedied by the adequate assignment of property rights. In particular, one may want to assign the property right over data (in particular, the right to conceal data) to individuals. Yet this assignment of property rights does not necessarily achieve efficiency.[39] It may be the case that the allocation is inefficient and does not even respond to the assignment of property rights. Thus, even without considering further complications on top of asymmetric information, a pure property rights approach to privacy appears to be ineffective.[40]

3.4. Beyond a property rights analysis

Pushing our economic analysis of privacy beyond this basic property rights analysis, we proceed in two steps. First, we lay out in more detail how the release of personal data affects market outcomes in certain environments (in particular, distinguishing between environments with a single or several competing firms). We identify situations in which the use of personal data by firms are, or are not, in the interest of individuals and society at large. Second, attention will be directed towards externalities and behavioural biases.

[38] See J. Hirshleifer 'The private and social value of information and the reward to inventive activity' (1971) 61 American Economic Review 561 and C. Taylor 'Privacy and information acquisition in competitive markets' Unpublished manuscript, Duke University (2005).
[39] B. Hermalin and M. Katz 'Privacy, property rights and efficiency: The economics of privacy as secrecy' (2006) 4 Quantitative Marketing and Economics 209.They show this in a simple setting with a single firm offering options to groups of individuals with price-sensitive demands, depending on the group characteristics which are obtained from analysing personal data. When individuals hold the property rights on personal data, the firm may refrain from offering its service if individuals do not disclose their personal data.
[40] This insight generalises to environments with many firms.

3.4.1. Privacy and market failures: information

Privacy policies may prohibit or inhibit the disclosure of information (or a firm's response to information). In general, such policies have efficiency and redistributive effects. In particular, the disclosure of information may allow firms to make better targeted offers. This tends to increase economic efficiency as larger gains from trade are realised. While both parties who are involved in a transaction may benefit, this result is not guaranteed. We elaborate on this point with some detail.

The tracking of previous purchases or search behaviour allows firms to make personalised offers. Firms may advertise a product to a particular group of consumers, or advertise the product among its portfolio which is most likely to match consumer preferences depending on the information available to the firm.[41] Of course, targeting may allow the firm to adjust its price. In particular, we may expect that if a firm is alone in a product category and is better able to match consumer preferences, it will optimally charge a higher price. In the extreme, the firm may not even provide a better match and simply personalise prices to consumer groups. Such personalised prices may be achieved through a uniform list price and targeted discounts. Then, knowing your customer better may allow for higher profits when the advertised product is the same for all consumers, as the firm can personalise its price according to the willingness to pay of specific consumers. This is a well-known result from the economics of price discrimination, which can be illustrated by a simple numerical example.[42]

Numerical example 1 (group pricing and targeting)

Suppose that there is a large number of consumers (say 100) who are interested in a particular good produced by one firm at zero costs per unit (there may be fixed costs). Consumers are assumed to have different valuations (willingness to pay), which are randomly drawn between 0 and 100. To keep things simple, each real number between 0 and 100 is equally likely. What does the firm optimally do to maximise its profits? Without further information about consumers, it has to offer the same price to all consumers. The profit-maximising price is 50, at which 50 consumers buy and, thus, the firm's profit is 2500.

Can the firm do better if it has additional information about consumers? Suppose that the firm does not perfectly know how much consumers value the product, but that it can distinguish two groups of consumers based on consumer data: it identifies those who are willing to pay more than 50 and those who are willing to pay less.[43] In this case the firm optimally charges 50 to those consumers belonging to the group with valuations over 50, and charges 25 to those

[41] A consumer may make inferences on the likelihood that a product will fit her tastes based on the context (an environment in which targeted advertising is practiced or where it is not), and possibly also on the content of an ad. B. Anand and R. Shachar 'Targeted advertising as a signal' (2009) 7 Quantitative Marketing and Economics 237 show that a firm may want to use targeted ads combined with advertising content.

[42] For an elaborate textbook treatment of the economics of price discrimination, see P. Belleflamme and M. Peitz, *Industrial Organisation: Markets and Strategies*, 2nd ed. (Cambridge: CUP, 2015).

[43] The argument holds more generally if the firm can identify consumers as belonging to a particular group and groups differ in their distribution of valuations.

belonging to the group with valuation less than 50. From the first group it makes a profit of 50 times 50 (= 2500) and from the latter of 25 times 25 (= 625) leading to an overall profit of 3125.

What this simple example shows is that by segmenting the market a firm can increase its profits. In the example, consumers benefit as well, since some consumers obtain the product at 25, who would not have bought at a uniform price of 50, absent that market segmentation. If the firm is able to even better segment the market (for instance, distinguishing 4 instead of 2 consumer groups) it can further increase its profits.[44] However, if the firm obtains a better and better guess of a consumer's valuation, consumers eventually do worse overall, since a larger fraction of the potential gains from trade are extracted by the firm. One may, therefore, be tempted to conclude that a firm necessarily benefits from the use of consumer data, while it is unclear whether consumers benefit, at least when a firm is on its own in a particular product category. This conclusion, however, is premature. It ignores the dynamic dimension: a firm learns from the behaviour of consumers about their valuations and consumer behaviour may be sensitive to such dynamic considerations. It is therefore useful to take another look at the numerical example above.[45]

Numerical example 2 (behaviour-based pricing and personal data).

We introduce dynamics in the simplest form into the above numerical example. Suppose that consumers consider buying the product in each of two periods (the product is short-lived and provides a value only for the concurrent period; such a situation also applies to subscriptions to a particular service for a particular period of time). The firm maximises profits as the sum of first-period and second-period profits and is able to track consumer behaviour, but lacks any other information on consumers. Thus, the firm will not have any information about consumers in the first period, but in the second period, the firm knows which consumers bought in the first period. If consumers make myopic decisions – i.e. they ignore in period 1 that they will again be active in period 2 – the firm can charge (i) 50 to all consumers in the first period and (ii) in the second period, the same price to those who bought in the first period and 25 to those who did not. The reason is that by buying the product in period 1, a consumer reveals that she has a valuation of at least 50. Thus, in the second period, we replicate the result from the numerical example above. The firm makes a profit of 3125 in the second period and a total profit of 5625. Here, being able to track consumers increases the firm's profits because otherwise the firm could only make a profit of 2500 in each period.[46]

However, this result may be questioned on the grounds that consumers may be forward-looking and understand the implications of their first-period behaviour. We take another look at the pricing of the firm presuming that the firm sets the prices for period 2 in period 2 (above we did

[44] See Belleflamme and Peitz, *supra*, note 41, chapter 8 for a short exposition.
[45] See also the exposition in Belleflamme and Peitz, *ibid.*, chapter 10. A more elaborate exposition is provided by D. Fudenberg and M. Villas-Boas 'Behavior-based price discrimination and customer recognition', in T. Hendershott, ed. *Handbooks in information systems: Economics and information systems* (Amsterdam: Elsevier, 2006).
[46] The firm can actually do better than this. It maximises its profit by setting a price slightly above 57 in the first period and the same price to consumers who bought in the first period and half this price to those who did not. Maximal profits are approximately 5714, with approximately 2449 in the first period and 3265 in the second.

not need to specify whether those prices are set in period 1 or 2). As we will see next, this has drastic consequences on the outcome. First, we see that with the pricing strategy which was optimal under consumer myopia, forward-looking consumers will behave differently. A consumer who decides whether to buy in the first period takes into account that this affects the second-period price he or she will face. Clearly, a consumer with a valuation slightly above 50 will not buy in the first period, since this will imply that she has to pay 50 in the second period, while she knows that she will face a price of 25 if she declines the offer in the first period. Hence, at a price of 50, fewer consumers will buy in the first period. This in turn implies that the firm will set different prices in the second period from the ones under consumer myopia. It will also lead to an adjustment of the first-period price.

Let us first consider the pricing period 2, when all consumers above some value *V* (greater than or equal to 50) have bought in period 1. Then the firm will charge *V* to consumers who bought in period 1 and half of *V* to those who did not. Thus, a consumer obtains her valuation minus the first-period price plus the difference between her valuation and value *V,* if she buys in the first period, while she obtains the difference between her valuation and half of *V,* if she does not buy in the first period. There is a critical consumer such that all consumers with higher valuation buy in the first period and all consumers with a lower valuation do not buy in the first period. When setting its first-period price, the firm takes into account how this critical consumer behaves, and the subsequent second-period prices depend on the first period price. Maximising its overall profits, the firm charges 30 in the first period. In the second period, the firm charges 60 to consumers who bought in period 1 and 30 to those who did not buy in period 1. With these prices, a consumer with valuation 60 is indifferent whether or not to buy in the first period.[47] All consumers with higher valuations buy in the first period. Thus, in period 1 the firm sells its product at price 30 to 40 consumers and makes a first-period profit of 1200. In period 2 it sells its product at price 60 to 40 consumers and makes a profit of 2400 from those consumers; it sells at price 30 to the remaining 30 consumers with valuation above 30 and makes an additional profit of 900. Hence, the firm makes a second-period profit of 3300, which is more than if it faced myopic consumers (3265), and also more than if it did not track consumers (2500). However, the firm's first-period profit of 1200 is much lower than what it would have been in the case where it did not track consumers and in the case of myopic consumers. Overall, the firm is worse off with consumer tracking (a profit of 4500) than if it did not track (a profit of 5000).

The general lesson that emerges from this example is that even if a firm is alone in its product category, with the ability to track consumers and make targeted price offers, it does not necessarily obtain higher profits once consumers behave with the knowledge that they are tracked (and infer second period prices). As illustrated, the firm would be better off if it could credibly convey to consumers that it did not seek to learn about consumer behaviour. Here, committing to a privacy policy may help the firm to commit not to track consumer behaviour,

[47] This is seen as follows: If this consumer buys in the first period her net surplus is 30 in the first period and 0 in the second. If she buys in the second period her net surplus is 0 in the first period and 30 in the second.

and thus may avoid a situation where the firm engages in price discrimination which runs counter to its own interests when it cannot commit to future prices.

So far we have focused on the use of personal data when a single firm sells a single product. Perhaps more interesting is an analysis that allows for multiple differentiated products. As alluded to at the beginning of this section, targeting may increase the fit between product and consumer tastes; it may also reduce the search cost a consumer incurs to find a product which provides a sufficiently good fit. Before addressing these two issues we explore some pricing implications when two firms compete with differentiated products.

Suppose that there are two firms in the market, which we call RED and BLUE, each offering a single product. Products are differentiated: at equal prices, some consumers prefer RED and others BLUE. If firms lack information about consumer tastes, they post a uniform price applicable to all consumers. As a result, each firm will set a price that allows for a positive profit margin, such that none of the firms gain from charging a different price. Consider now a situation where firms can learn whether consumers are RED or BLUE lovers. They can then make targeted offers to these two consumer groups. The BLUE firm is willing to sacrifice almost all its profit margin when making a targeted offer to RED lovers since it knows that it is at a disadvantage when competing for those consumers. The same applies for the RED firm with respect to BLUE lovers. The implication is that if both firms have access to this information, they will compete more fiercely than in the absence of information. In addition, each firm has an incentive to acquire this information. Hence, firms will acquire personal data at some cost and obtain lower profits even when abstracting from those costs. Again we are in a situation in which firms would benefit from a stringent privacy policy, which does not allow them to extract information on consumer tastes. Here, it is of no help if one firm implements such a privacy policy on its own initiative. Rather, it benefits from the competitor doing so. Therefore, firms may lobby for a privacy policy to be implemented through self-regulation or government intervention.

While our example suggests that competition tends to be more intense when firms have access to personal data of consumers, we should not conclude that all consumers necessarily benefit, because consumers who are very attached to a particular product configuration may end up paying more than under uniform pricing. Also, we should not conclude that more intense competition necessarily improves the allocation. Indeed, it is not in the interest of society if some BLUE lovers buy from RED and vice versa. If firms do have some, but not very precise, information about consumer tastes, we must expect such a situation to arise. Therefore, starting in a situation in which firms do not possess any information about consumer tastes, obtaining more information may actually lead to an inefficient allocation.

Similar to our two-period example with a single firm and a single product (numerical example 2 above), we may ask what happens if firms have to track consumer behaviour to make inferences about consumer tastes in a subsequent period. If we consider a two-period setting in which the firms, in the first period, lack any information about consumer tastes, each firm initially sets one price for all consumers. A consumer who buys from BLUE and not from RED (at similar prices) reveals to the firms that she is a BLUE lover because otherwise she would have bought RED. In

this way firms learn from consumer behaviour in period 1 to which group a consumer belongs. However, as suggested above, we need to be a bit more careful here. Some consumers are strong BLUE lovers, others may have only a slight preference at equal prices. If, in line with numerical example 2, firm BLUE decides to offer a lower price than RED in the first period, it then not only attracts BLUE lovers, but also those RED lovers with only a weak preference for RED. By attracting more consumers in the first period, a firm invites tougher competition in the second period. Effectively, firms are inclined to compete fiercely on price in the second period with consumer tracking. However, this renders consumers less valuable for firms in the first period. Consequently, firms compete less fiercely in the first period. This leads to initially higher prices and may actually harm consumers overall.[48]

We return to the situation of a single firm, but now postulate that a firm has the option of offering personalised products. Personalised products increase the match quality, yet we may wonder if it is indeed in the interest of a firm to provide an improved match. The following simple numerical example sheds some light on the issue.

Numerical example 3 (targeted advertising, match quality and versioning)

Suppose that there is a single firm in a particular product category. Using the same terminology as in the example above, we postulate that there are BLUE lovers and RED lovers in the population. For the moment we do not consider lovers of varying degrees and it is sufficient to have identical consumers in each of the two groups. There are 50 BLUE lovers and 50 RED lovers. The firm can offer a single non-customised product, which we call BLAND. All consumers have valuation 50 for BLAND. The firm also has the option to offer customised products BLUE or RED (it may choose any combination of products). BLUE lovers are assumed to have valuation 80 for BLUE and 0 for RED and vice versa for RED lovers. Thus, if the firm lacks any information about consumer tastes and consumers randomly select a single product among those on offer (they lack the time or resources to consider more than one product; alternatively, the firm can only send a single ad to each consumer) it is best for the firm to offer only BLAND and charge a price of 50. All consumers will buy and the firm obtains a profit of 5000.

Suppose now that the firm has access to consumer data that makes it possible to tell RED lovers from BLUE lovers. It can target an ad announcing a different product depending on the consumer type. Even though this opens up new possibilities, the firm can replicate the strategy of an uninformed firm and sell the BLAND product to all consumers at price 50. However, it can do better and offer BLUE to BLUE lovers and RED to RED lovers and charge a price of 80. All consumers will buy and the firm makes a profit of 8000. This shows that the firm benefits from offering customised versions to respective customer groups through the use of targeted advertising.

[48] This is the key insight from D. Fudenberg and J. Tirole, 'Customer Poaching and Brand Switching' (2000) 31 Rand Journal of Economics 634. For a textbook treatment, we again refer to Belleflamme and Peitz, *supra*, note 41, chapter 10.

The example does not provide any meaningful guidance on how to view customisation and tailored advertising from a consumer perspective, since the firm is able to extract all expected surplus. Whether consumers gain or lose from targeting and customisation depends on the dispersion of consumer tastes, with and without the availability of consumer data. Consumers are better off from targeted advertising if consumers in the target group have more heterogeneous tastes about the targeted product than the whole consumer population about the BLAND product. To see this, we slightly modify the example and introduce 'weak' and 'strong' lovers of the two customised products. Suppose that, of the 50 BLUE lovers, 25 have valuation 85 and 25 have valuation 75 for BLUE; all these consumers continue to have valuation 0 for RED and 50 for BLAND. This holds vice versa for RED lovers. Now the firm sets a price of 75 after customisation and targeting and obtains a profit of 7500. Half of BLUE lovers and half of RED lovers (those with the highest valuation, at 85) are strictly better off when the firm sells customised products with targeted advertising. Thus, in this example, both consumers and the firm benefit from customisation and targeting.

The above example shows that firms tend to be interested in improving match quality and offering customised products, if they can make use of personal data. Whether consumers benefit from such actions cannot be unambiguously determined. However, since customisation increases total surplus, consumers will benefit as long as the fraction of the surplus that goes to consumers does not decrease with targeting and customisation (in the numerical example it increases from zero to some positive fraction). Mandatory privacy rules may have the consequence that targeting and customisation will be hampered to the detriment of firms, society, and also, depending on the situation, consumers.

In the above examples, consumers hold personal data. If this information is not disclosed, a firm faces an asymmetric information problem, as it cannot assess which products are of interest to the consumer in question. So far we ignored the possibility that a firm's profit is directly affected by the consumer type, conditional on the consumer buying a product. However, this is not always the case. For instance, a bank providing a loan is interested in the default risk of a particular client, which is likely to be correlated with certain personal data. Here, privacy protection that makes it impossible for a bank to gather the relevant data may lead the bank to be more restrictive in its lending, as it faces the problem that it collects bad risks. A similar issue occurs for an online retailer who has some customers who are very likely to return products which then have to be sold at a loss.[49] A related point can be made, when monitoring the activity of a consumer provides incentives for the consumer not to take actions which are not in the interest of the firm; e.g. in the case of an insurance contract, engaging in activities which are likely to lead to a loss.[50]

[49] The situation of private information and resulting adverse selection has been explored at depth in economics. In the extreme, such asymmetric information problems can lead to market breakdown. Thus (some) information disclosure may be needed for a market to be active. See further below on this.

[50] This is an instance of moral hazard. Monitoring in repeated interactions with moral hazard provides incentives to avoid socially inefficient activities. This monitoring relies on information disclosure (in particular, tracking of past behaviour) and possibly information sharing among firms.

What the analysis of information disclosure in a context of otherwise asymmetric information tells us, is that firms and consumers often benefit as the quality of matches between products and services on one side, and consumer tastes on the other side, increases or the cost of achieving those matches is reduced. However, it cannot be taken for granted that both benefit; firms or consumers may suffer from the disclosure of personal data. While this provides some grounds for privacy regulation, we are on a slippery slope, since, in many situations, firms and consumers would suffer from restrictions arising from privacy regulation. It suggests that indiscriminate restrictions of the acquisition and use of personal data, based on a standard market failure argument, are likely to be detrimental to consumers and society at large and a more flexible regulation is needed.[51]

3.4.2. Privacy and market failures: externalities

Information disclosure may not be in the interest of consumers generally, even if it is individually rational. One reason relates to differential prices, as has been discussed above. Another reason is externalities: The release of private information may not only reveal information about an individual, but also about other individuals. For instance, if tastes are correlated within family or a group of friends then learning about the preferences of an individual also provides valuable information on her family or friend network. An individual may have received a reward for providing this information, but she may ignore the negative (or positive) externality this exerts on her friends or family.

An extreme example of such externalities (which can be positive or negative) across family members is genetic testing. Here disclosure of personal data may not only negatively affect the individual who provided her data to some party (e.g. a hospital), but also some family members.

However, there are also positive externalities for society at large if information collected from genetic testing allows for the development of new treatments or a more efficient allocation of budgets for medical research. Privacy laws can affect not only the disclosure behaviour of individuals but also to which extent individuals generate personal information (in the above example, the inclination of individuals to undergo genetic testing).[52] Here, clear privacy laws or alternative mechanisms that generate trust on the consumer side may actually increase the quality of information available to the data collector, as consumers otherwise refrain from participating.

A further insight concerns the sharing of highly disaggregated data. In instances of positive externalities, society would like more personal data to be collected and these data (in anonymised form) to be made widely available. To elaborate on this insight, consider another

[51] Specific recommendations for privacy regulation - this includes the encouragement to privately develop privacy standards (in the form of codes of conduct or trustmarks) - are developed in Section 5.
[52] Genetic testing may, in particular, be used to assess individual cancer risks. A. Miller and C. Tucker, 'Privacy protection, personalized medicine and genetic testing', Mimeo (MIT, 2014) provide an empirical assessment of the effect of different privacy laws (that have been adopted by different U.S. states) on the diffusion of personalised medicine.

example in a health context: search items on search engines combined with location data can help in predicting outbreaks and developments of infectious diseases (e.g. Google Flu Trends provides information on influenza-related searches), which in turn helps in directing efforts and resources to contain the disease. Health authorities may be interested in these detailed data. A different example is GPS information (that also communicates traveling speed and destination) by car users (e.g. as used by Waze), which can help in managing traffic flows and reduce overall traffic congestion. In such situations, society benefits from detailed data becoming widely available. In general, such data can (and should) be anonymised. However, anonymisation is not always a safeguard and it is possible that some individuals can be identified. Therefore, if data collectors run legal risks, they may be hesitant in making anonymised big data at a disaggregate level available to third parties, to the detriment of society

3.4.3. Privacy and behavioural biases

While asymmetric information and externalities are important aspects in the analysis of public policy on privacy, arguably the most important reason for the introduction of privacy regulation is behavioural biases and imperfect decision-making, such that individuals choose actions that are not in their long-term interest.[53]

A large economic literature on behavioural biases and imperfections in individual decision making is directly relevant in the context of privacy. Instances of such behavioural biases and imperfect decision making are: (i) individuals may be unaware of some of the future consequences of their behaviour (which is different from simply being uncertain), (ii) individuals may have a present bias and not take future costs or losses appropriately into account,[54] (iii) individual behaviour may respond to framing, i.e. the way in which a disclosure option is presented, and (iv) individuals may simply make mistakes when taking an action (e.g. accidentally clicking the wrong box). While the literature has identified circumstances in which individuals make choices that are incompatible with rational decision making, it is less clear *a priori* which of these explanations are the most relevant in the privacy context. For this, we have to take a closer look at the issue.

As a starting point, there appears to be a disconnect between privacy attitudes and individual behaviour – the so-called 'privacy paradox'. The privacy paradox plays out for instance with regards to targeted advertising. A vast majority of people (in the U.S. and elsewhere) use search engines and social networks; the personal data collected in that process enables targeted advertising. At the same time, many individuals state that they do not wish to receive targeted ads.[55] One response to such an alleged privacy paradox is that while individuals are against

[53] A. Acquisti, L. Brandimarte, and G. Loewenstein 'Privacy and human behavior in the age of information' (2015) 347 Science 509 provide a useful discussion and overview.
[54] A. Acquisti, 'Privacy in electronic commerce and the economics of immediate gratification', in [2004] Proceedings of the 5th ACM Conference on Electronic Commerce 21.
[55] According to a survey by J. Turow et al. 'Americans reject tailored advertising and three activities that enable It'. unpublished manuscript, available at http://repository.upenn.edu/asc_papers/137 (2009), roughly two thirds of Americans do not wish to receive targeted ads.

targeting and personalisation, their opportunity cost is rather low and they accept proposals to disclose personal data if doing so provides a small benefit (using a service for free, or even not having to bother with changing default options in privacy settings). A recent survey by PEW Research Center confirms that while a majority is against personalisation, a majority is also willing to make trade-offs to receive a 'free' service.[56]

A starker difference between attitude and behaviour is reported in the context of information disclosure on Facebook.[57] A subgroup of participants expressed a major concern if their sexual orientation, political views or partner's name becomes known to strangers. Yet, a substantial fraction of that subgroup publicly disclosed this information in the social network.[58]

There is direct evidence that behavioural biases can strongly affect the value assigned to the protection of personal data and the disclosure decision. Depending on the framing of the trade-offs when disclosing personal data, the value can vary considerably.[59] Similarly, framing affects the likelihood that individuals disclose personal data.[60]

To interpret some of the empirical findings properly, we note that privacy concerns and behavioural biases depend on time and space. One instance of survey evidence on a change of privacy concerns over time is uncovered by Goldfarb and Tucker.[61] A respondent's privacy concern is measured by her unwillingness to disclose income; on average privacy concerns were increasing over an 8-year period. Attitudes may depend on social norms which both evolve over time and depend on a particular community. Also, the type of personal data which is deemed to be sensitive may vary over time and space.

Behavioural biases lead to individually suboptimal choices. In general, privacy regulation should remedy misallocations due to behavioural biases, especially if these biases are persistent. Individuals may be tricked into providing sensitive information, which may be directly exploited by firms (and, if not properly protected by the firm, disclosure may also lead to unforeseen risks of misuse by others). Privacy policies try to limit such actions.

Even absent privacy regulation, one corrective force may be a public outcry about the way personal data are used or are planned to be used, possibly followed by a consumer boycott. However, it may take individuals too long to figure out what is going on and the public outcry may prove ineffective. Thus, such a public response appears to be a poor substitute for

[56] As Pew Research Center 'Public perceptions of privacy and security in the post-Snowden era' (2014) available at http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/reports, "61% of adults 'disagree' or 'strongly disagree' with the statement: 'I appreciate that online services are more efficient because of the increased access they have to my personal data.' At the same time, 55% 'agree' or 'strongly agree' with the statement: 'I am willing to share some information about myself with companies in order to use online services for free.' "
[57] A. Acquisti and R. Gross 'Imagined communities: Awareness, information sharing, and privacy on Facebook', in G. Danezis and P. Golle, eds. *Privacy enhancing technologies* (Springer, 2006).
[58] The numbers are as follows: 48% publicly disclosed their sexual orientation, 47% their political views, and 21% their partner's name.
[59] A. Acquisti, L. K. John, and G. Loewenstein 'What is privacy worth?' (2013) 42 Journal of Legal Studies 249.
[60] L.K. John, A. Acquisti, and G. Loewenstein 'Strangers on the plane: Context-dependent willingness to divulge sensitive information' (2011) 37 Journal of Consumer Research 858.
[61] A. Goldfarb and C. Tucker 'Shifts in privacy concerns' (2012) 102 American Economic Review (Papers and Proceedings) 349.

providing privacy regulation that limits the misuse of personal data. Privacy regulation ideally reflects the public discourse of what constitutes a legitimate acquisition and use of personal data. [62] It thus also provides a predictable framework for the design of a firm's privacy policy.

3.5. Lessons from the economics of privacy

The general take-away that emerges from the economic analysis is that the suspicion that the disclosure of personal data typically makes consumers worse off is unfounded. In many situations, consumers and firms alike benefit from personal data being available and used by firms for commercial purposes. This report has documented economic arguments that support this conclusion. However, results are nuanced in the sense that the commercial use of personal data is not unambiguously positive and can potentially harm consumers and society. A strong case in favour of privacy regulation can be made when consumers suffer from persistent behavioural biases. Here, a minimum standard of privacy can protect consumers who otherwise would be disadvantaged from disclosure.

[62] Ideally, they are reflected in principles of privacy regulation; see Section 4 for principles in EU regulation.

4. The legal approach to privacy and data protection in Europe

Against the background that the commercial use of personal data may require some regulation from an economics perspective, this section gives a brief account of the legal approach to the information privacy in Europe, including a comparison with US policy.

4.1. Agreeing on terms: privacy, information privacy and data protection

The right to respect for private life and data protection are often referred to as 'privacy rights'. The two rights are related and significantly overlap. At the same time, they are not the same. The right to respect for private life, as protected by Article 8 of the European Convention of Human Rights, covers a broad range of privacy interests, from the protection of home, family life and correspondence to bodily integrity and decisional autonomy. In part related to personal information, the right to respect for private life is often referred to as the right to information privacy and is characterised as an 'opacity tool', meant to shield one's private sphere from the gaze of others; the State in particular, but also private actors. In contrast, the right to data protection is characterised as a 'transparency tool', meant to empower the individual to control how others collect and use information about him / her, e.g. by means of information and other control rights.[63] In the US the term 'information privacy' is used instead of, and in the meaning of, the European term 'data protection.' This report will use 'information privacy' in the meaning equivalent to 'data protection'. The two terms will be used interchangeably, unless specifically stated otherwise.

4.2. What we mean by a 'European approach'

When talking about a 'European' approach to information privacy, scholars and policymakers often refer to the approach taken on the European continent by the most significant European institutions - the European Union and the Council of Europe. 'The European approach' to privacy and data protection is often contrasted with the approach taken in the United States.

This report understands the European approach to privacy and data protection as the approach of the European Union and the Council of Europe. Despite still present and numerous differences between EU Member States, they share significant common goals such as the creation of an internal market, traditions of regulation and the system of human rights protection. Importantly, they also share a common policy on data protection expressed, inter

[63] P. De Hert, "Making Sense of Privacy and Data Protection: A Prospective Overview in the Light of the Future of Identity, Location-Based Services and Virtual Residence" Annex I in Institute for Prospective Technological Studies, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview* (Report EUR 20823 EN, 2003).

alia, in the Council of Europe Convention No. 108 for the protection of individuals with regard to the automatic processing of personal data[64] (Convention 108) and the EU Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data ('the DPD').[65] Although some differences are still present between the individual Member States in how they implement Convention 108 and the DPD, these instruments may be said to present a unified approach which is sufficiently coherent to qualify as a 'European approach'.

In principle, this coherency should only be increased with the enactment of the GDPR, which will be directly applicable in the laws of the Member States by virtue of being a regulation. In January 2012 the Commission proposed a new General Data Protection Regulation ('Commission Proposal').[66] In October 2013 the Committee on Civil Liberties, Justice and Home Affairs ('LIBE Committee') adopted its compromise text amending the Proposal ('LIBE compromise text'),[67] and the Parliament adopted it in the first reading. Most recently, the Council reached its general approach to the proposed regulation on 15 June 2015 ('Council general approach').[68] The discussions in the Parliament, Council and the Commission to complete the reform effort are scheduled to take until the end of 2015.[69] In the following overview, the discussion of the draft GDPR is based on the Council general approach, unless otherwise indicated.

4.3. 'The European approach' as contrasted with the US approach

The 'European approach' to information privacy and data protection is often contrasted with the approach taken in the United States. Indeed, these two approaches have emerged from different regulatory cultures and have been conditioned by the constitutional and political constraints of both systems, which often led to different results as to the scope and the means of privacy protection.

4.3.1. The human rights approach in Europe vs limited constitutional protection in the US

The European approach is often said to be 'rights-based', meaning that information privacy and data protection are fundamental rights, enshrined in constitutional instruments at European and national levels, and often originating from other constitutional values, such as human dignity

[64] Adopted by the Committee of Ministers of the Council of Europe on 28 January 1981.
[65] Directive 95/46/EC of 24 January 1995 [1995] OJ L 281/31.
[66] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final – 2012/0011 (COD), 25.01.2012.
[67] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf and http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf.
[68] available online at www.data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf
[69] http://www.eppgroup.eu/news/Data-protection-reform-timetable

and self-determination.[70] This is different from the US where – at least on the federal level – the role of the Constitution and constitutional rights in privacy protection is limited.

The rights to privacy and to data protection became generally recognised as a part of the national constitutional heritage of most EU Member States,[71] often as two separate rights and sometimes as parts of an overarching constitutional right to privacy, autonomy, or development of personality. For instance, data protection rights in Belgium have a constitutional basis in the right to respect for private life, deemed to include protection in cases of data collection, registration, use and transfer.[72] German data protection has evolved from the value of human dignity and a right of development of personality. The German Basic Law does not contain explicit provisions on privacy or data protection. However, both have been read into *the general right of personality*, which evolved from the constitutional value of human dignity.[73] Data protection rights have become a part of the Dutch Constitution as a result of the 1983 Constitutional revisions, when they were *attached* to the general right to privacy at Article 10.[74]

A similar 'constitutionalisation' of the rights to privacy and data protection has taken place at EU level: the EU Charter of Fundamental Rights protects both the right to respect for private and family life (Article 7) and the right to protection of personal data (Article 8). Article 16 TFEU introduces the right to data protection and instructs the EU institutions to take legislative steps to effectuate this right throughout the Union law.

Although the language of the European Convention on Human Rights does not explicitly recognise the right to data protection, and the relevant Article 8 only defines the scope and limitations of the right 'to respect for private and family life,' the case law of the European Court of Human Rights already explicitly brought a number of data protection rights under the protection of Article 8 in cases involving interception of communication,[75] surveillance[76] and protection against storage of personal data by public authorities.[77] Under Article 8 of the ECHR, the states are not simply obliged to refrain from active violations of Article 8 rights, but are also

[70] Such as in Germany.
[71] B.-J. Koops, 'Conclusions and Recommendations', in R. Leenes, B.-J. Koops and P. De Hert, eds., *Constitutional Rights and New Technologies: A Comparative Study*, (The Hague: Asser Press, 2008) 271.
[72] Article 22 of the Belgian Constitution: E. Lievens et al., 'Constitutional Rights and New Technologies in Belgium', in R. Leenes at al., *ibid.,* 25.
[73] Article 2(1) read together with Article 1(1) of the *Grundgesetz* (Basic Law). T. Hoeren & A. Rodenhausen, 'Constitutional Rights and New Technologies in Germany', in R. Leenes at al., *ibid.* 39 referring to the decision of the Federal Court of Justice (*Leserbrief*) later adopted by the Federal Constitutional Court (*Elfes-Urteil* decision).
[74] B.-J. Koops & M. Groothuis, 'Constitutional Rights and New Technologies in the Netherlands', in R. Leenes et al., *ibid.*, 166. Paragraphs 2 and 3 of Article 10 of the Dutch Constitution contain respectively the instructions to the Parliament to pass a law protecting privacy 'in connection with the recording and dissemination of personal data'; and to establish individual rights 'to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected'
[75] ECtHR, *Malone* v. *United Kingdom*, No. 8691/79, 2 August 1984; ECtHR, *Copland* v. *United Kingdom*, No. 62617/00, 3 April 2007.
[76] ECtHR, *Klass* v. *Germany*, No. 5029/71, 6 September 1978; ECtHR, *Uzun* v. *Germany*, No. 35623/05, 2 September 2010
[77] ECtHR, *Leander* v. *Sweden*, No. 9248/81, 26 March 1987; ECtHR, *S.* v. *United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008.

under positive obligations to take measures to secure effective respect for these rights.[78] Some European privacy and data protection scholars argue that there are sufficient grounds to treat data protection interests in general as an integral part of a right to respect of private life.[79] Thus, in Europe a discussion of information privacy and data protection is unavoidably a human rights discussion.

Similarly, in the US the origins of privacy lie in the American Constitution and its Bill of Rights, in particular the Fourth Amendment right against unlawful search and seizure.[80] Beyond that, however, the role of the Constitution and hence the human rights aspect of information privacy is much more limited in the US. In a large part this is due to the nature and function of the Constitution, which is to establish the federal government and to protect the American people and their liberty from tyranny by imposing limits on government powers.[81] This has a number of major implications for the federal Constitutional protection of privacy in the US:

- First, constitutionally protected privacy interests only impose restrictions on the actions of the federal (and later state) governments, and do not affect the data processing practices of private entities.[82]
- Second, the Constitution only prevents the government from acting in certain ways, but does not create any positive duties, including the duty to create a system of data protection rules applicable to information use by the government.[83]
- Third, the Constitution does not establish a baseline of information privacy protection.
- Fourth, the emphasis is on limiting the government rather than regulating behaviour of citizens. Since communication of information enjoys constitutional protection in the First Amendment (freedom of speech), this results in "a basic regulatory philosophy that favours the free flow of information",[84] and imposes restrictions on any legislative initiatives to

[78] ECtHR, *I.* v. *Finland*, No. 20511/03, 17 July 2008; ECtHR, *K.U.* v. *Finland*, No. 2872/02, 2 December 2008.
[79] Among others, N. Purtova 'Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights' (2010) 28 Neth Q Human Rights 179; D.J. Harris et al., *Harris, O'Boyle & Warbrick Law of the European Convention on Human Rights*, 2nd edn (Oxford University Press, 2009) at 361 ("Private life thus extends beyond the narrower confines of the Anglo-American idea of privacy, with its emphasis on the secrecy of personal information and seclusion").
[80] J.Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 Yale L.J. 1151 at 1211-1212. See also K. Gormley, 'One Hundred Years of Privacy' [1992] Wisconsin L. Rev. 1335 at 1358-1359, explaining that "if privacy was explicitly acknowledged anywhere in the early contours of American law, it was within the folds of criminal procedure, where … there existed a strong principle, inherited from English law, that a "man's house is his castle; and while he is quiet, he is well guarded as a prince in his castle." … Such a fierce protection of the inner sanctum of the home therefore made its way into the US Constitution in the fashion most relevant to citizens of the early American period. A prohibition against the quartering of soldiers was placed in the Third Amendment;… A requirement of particularized warrants to guard against unreasonable searches and seizures was embodied in the Fourth Amendment."
[81] P. Schwartz and J.R. Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (Charlottesville: Michie, 1996) at 6.
[82] D.J. Solove, 'Privacy and Power' (2001) 53 Stanford L Rev 1393 at 1435; Schwartz and Reidenberg, *ibid.*, 6.
[83] Solove, *ibid.*
[84] Schwartz and Reidenberg, *supra,* note 80.

regulate processing of personal data by private persons and entities.[85] Perhaps as a consequence of this, the general approach in the United States is to allow personal data processing unless it causes a legal harm or is otherwise restricted by law, while in Europe no processing of personal data is possible unless there is a legal basis.[86]

The US Constitution does not explicitly protect information or any other privacy right. The constitutional protection of some aspects of privacy is based on the interpretation of a number of constitutional amendments by the US Supreme Court: the Substantive Due Process Clause of the Fourteenth Amendment, the Fourth Amendment prohibition of unreasonable searches and seizures, and the Fifth Amendment right not to incriminate oneself. When applied in the information privacy context, these amendments have been invoked to prevent the government 'from carrying out certain kinds of collection, utilisation and disclosure of personal information'.[87]

The Substantive Due Process clause of the Fourteenth Amendment has been traditionally used to safeguard rights that are not otherwise enumerated in the Constitution.[88] The clause became relevant for privacy protection after the US Supreme Court found, starting with cases involving contraception and abortion, that the notion of privacy is covered by the concept of personal liberty protected by the Fourteenth Amendment.[89] In 1977 in *Whalen v. Roe*,[90] the Supreme Court extended its substantive due process privacy protection to personal data, and shaped what is often referred to as the 'constitutional right to information privacy',[91] also worded as 'the individual interest in avoiding [the] disclosure of personal matters'.[92]

The Fourth Amendment provides protection to 'persons, houses, papers, and effects, against unreasonable searches and seizures'. It provides that 'no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized'.[93] The Amendment has been recognised as significantly limiting the power of the government to collect data as a form of search or seizure.[94] In *Katz v. United States*[95] the court explained that 'what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in the area accessible to the public, may be

[85] Solove, *supra*, note 81 at 1458, explains that any such attempt to regulate 'may run into First Amendment problems'.
[86] P. Schwartz and D.J. Solove, 'Reconciling Personal Information in the United States and European Union' (2014) 102 California L Rev 877, citing P. Schwartz 'Preemption and Privacy' (2009) 118 Yale LJ 902 at 913–14.
[87] Schwartz and Reidenberg, *supra*, note 80, 29.
[88] E. Chemerinsky, 'Substantive Due Process' (1999) 15 Touro L Rev 1501 at 1505 et seq.
[89] *Griswold* v. *Connecticut* 381 US 479 (1965); *Roe* v. *Wade* 410 US 113 (1973) at 153.
[90] *Whalen* v. *Roe* 429 US 589 (1977); Justice Brennan, concurring, explained: '[Broad] dissemination by state officials of such information … would clearly implicate constitutionally protected privacy rights, and would presumably be justified only by compelling state interests.' at 606.
[91] D.J. Solove, M. Rotenberg and P. Schwartz *Information Privacy Law*, 2nd ed. (Aspen Publishing, 2006) at 400.
[92] *Whalen* v. *Roe* 429 U.S. 589 (1977).
[93] US Constitution, Fourth Amendment.
[94] Solove at al., *supra* note 90 at 208.
[95] *Katz* v. *United States* 389 US 347 (1967)

constitutionally protected'.[96] The decision established a widely used *reasonable expectation of privacy* test for privacy violations under which the Fourth Amendment affords protection if (a) a person exhibits an 'actual (subjective) expectation of privacy' and (b) 'the expectation [must] be one that society is prepared to recognise as 'reasonable'.[97] The *Katz* ruling is also the foundation for not granting any constitutional protection regarding personal information once it is disclosed to a third party, such as a social networking site.

The Fifth Amendment establishes a privilege against self-incrimination and prohibits the government from compelling individuals to disclose incriminating information about themselves. This way the Fifth Amendment limits the government's power to collect data from its citizens about themselves.[98] However, the same Amendment does not prevent the authorities from subpoenaing the same information from third parties.[99]

4.3.2. Cross-sectoral protection in Europe vs piecemeal sectoral protection in the US

It is often written that the European approach to information privacy and data protection is embodied in an omnibus law of cross-sectoral relevance (the 1995 Data Protection Directive), whereas the US approach is piecemeal, granting uneven protection across sectors.

Whereas the European system of information privacy and data protection is a hierarchical system with the constitutional values of the respective rights on top, and the supranational EU and national instruments below them, US information privacy law does not have a single, hierarchical order of rules. Instead the privacy protection there is comprised of a patchwork of rules from different sources, pertaining to different subjects of regulation and applicable in different contexts: tort, constitutional law and statutes.[100] In addition, the US privacy protection functions in the country's federalised legal system, where the competence to act is divided between the federal government and the States.[101]

One key characteristic of the US approach to privacy – arguably reflecting the lack of comprehensive protection – is the difference in protection between the public and private sectors. For reasons having to do with the US constitutional tradition described above, public and private sector data protection have been treated separately. On the one hand, the public sector is covered by the 1974 Privacy Act.[102] On the other hand, private sector data processing is

[96] Ibid.
[97] Ibid.
[98] Solove et al., *supra* note 90 at 208.
[99] The Supreme Court explained that 'the Fifth Amendment privilege is a personal privilege: it adheres basically to the person, not to information that may incriminate him' (*Couch v. United States* 409 US 322 (1973)).
[100] This piecemeal nature appears clearly in *Schrems*, discussed *supra.*
[101] Schwartz and Reidenberg, s*upra* note 80 at 7–8.
[102] Although the Privacy Act does cover most records maintained by state and local officials, it also has a wide range of other exceptions. For a more detailed analysis of the Act, see Rotenberg (Ibid.) who argues that, provided a few gaps are filled in, the Privacy Act is a satisfactory data protection tool in the public sector; Bignami 'The U.S. Privacy Act in

almost entirely left to self-regulation, albeit with the exception of a number of statutes, like the Video Privacy Protection Act of 1988 and the Right to Financial Privacy Act of 1978, both of which were adopted as a reaction to particularly shocking incidents of data mishandling.[103] The federal Health Insurance Portability and Accountability Act (known as HIPPA) adopted in 1996 establishes rules for processing health data, but only in given contexts and by a limited group of actors. The Children's Online Privacy Protection Act of 1998 (referred to as COPPA) sets out some rules on processing of personal data online, but again this instrument does not create an overarching regime of online privacy for children: for instance, the protection is limited to children under the age of 13, and directed against *commercial* website operators *intentionally* collecting personal information, etc.[104] As a result, only some areas of data processing are covered by statutory protections, whereas others are unaddressed.

In addition to statutory law, US tort law (civil liability) is also relevant for information privacy protection in the private sector. It is sometimes said that tort law played a ground-breaking role in the protection of privacy in the US.[105] The doctrinal foundations of the legal protection of privacy were laid down by Warren and Brandeis[106] (who described privacy as 'the right to be left alone') and were since picked up in the case-law. There are four torts pertaining to privacy: (1) intrusion upon a plaintiff's seclusion or solitude, or into his private affairs; (2) public disclosure of embarrassing private facts; (3) publicity which places one in a false light in the public eye; and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[107] However, the protection granted by these four torts is limited to personal information that has not been disclosed, or to protection against publication of false information. In addition, actions under these torts only succeed when observable damages have been incurred. Hence, the privacy torts are of limited significance in restraining the modern-day data processing practices where data is in principle accurate, data processing is often more opaque than public, and damages are difficult to observe and the harm is caused to society.[108]

In summary, and in contrast to the EU's comprehensive umbrella data protection legislation, it is customary to describe the US approach to regulation of private sector personal data processing

---

Comparative Perspective', Contribution to the EP Public Seminar 'PNR/SWIFT/Safe Harbour: Are Transatlantic Data Protected?' (2007), discusses the weaknesses of the Act.

[103] 'The number of laws does not reflect [the] enormous policy success by privacy advocates. Some of these laws, notably the Video Privacy Protection Act of 1988 and the Right to Financial Privacy Act of 1978, were passed in response to specific circumstances that highlighted threats to privacy. But more importantly, the actual number of laws passed pales in comparison to the amount of congressional activity devoted to the subject and the number of laws not passed, involving, for example, medical privacy, personality tests, the sale of personal information, and the use of the social security number.' P.M. Regan, *Legislating Privacy* (Chapel Hill: University of North Carolina Press, 1995) at 5–7.

[104] See D.R. Hostetler and S.F. Okada 'Children's privacy in virtual K-12 education: virtual solutions of the amended Children's Online Privacy Protection Act (COPPA) Rule' (2013) 14 North Carolina J L Tech 167.

[105] Solove et al., *supra* note 90 at 9.

[106] S.D. Warren and L.D. Brandeis 'The Right to Privacy' (1890) 4 Harv L Rev 193.

[107] P. Prosser 'Privacy' (1960) 48 Cal L Rev 383 at 389.

[108] N. Purtova, *Property in personal data: a European perspective* (Deventer: Kluwer Law International, 2011) Chapter 5, section 3.1.; V. Bergelson, 'It's Personal, but Is It Mine? Toward Property Rights in Personal Information' (2003) 37 UC Davis L Rev 379 at 405; see also Solove, 'Privacy and Power', p. 1432

as reactive rather than anticipatory, ad hoc or incremental rather than systematic and comprehensive, and fragmented rather than coherent.[109] Where the laws and regulations are absent, the private entities employ tools of self-regulation, such as codes of conduct, trust marks and certification, privacy policies and so on.

4.3.3. Convergence of the EU and US approaches

In the end, the observed divergences are to a large extent due to different constitutional and political contexts, and concern means rather than ends. On the fundamentals, US and European approaches to privacy are not far apart. Both systems see the origins of privacy in the idea of personal liberty and autonomy.[110]

In addition, the two systems are increasingly showing convergence in the regulation and enforcement of information privacy. The two most notable convergence trends are the role of the Federal Trade Commission to police deceptive and unfair commercial practices, growing closer to the role that the European data protection authorities play in the application and enforcement of the EU data protection law;[111] and a growing reliance, in EU data protection law, on private instruments (self-regulation and codes of conduct, certification and privacy seals, etc.).[112]

4.4. Elements of the EU Data protection regime

Data protection law may be viewed as a combination of substantive rules and principles, and implementation mechanisms, together creating an operational mechanism of data protection.

4.4.1. The substantive rules and principles

The substantive rules and principles of data protection reflect normative choices made in the EU as to how, and under what circumstances, personal data may be processed. They include general data protection principles, grounds of legitimate data processing applicable to all personal data, and special regimes for processing so-called 'sensitive' categories of personal data and for data transfers outside the EU.

General principles of data protection (Article 6 DPD) include fairness and lawfulness (data may be processed only when lawful grounds and other statutory conditions of processing are met),

[109] See, e.g. Regan, *Legislating Privacy*, pp. 5–7, Colin J. Bennett, 'Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?', in *Technology and Privacy: The New Landscape* ed. Philip E. Agre & Marc Rottenberg (Cambridge, Massachusets: MIT Press, 1997), Solove, *supra* note 81 at 1440.
[110] Regarding the US, see J. Cohen "What privacy is for" (2013) 126 Harvard L Rev 1904 at 1906 et seq.; regarding the European foundations of privacy in autonomy – e.g. A. Rouvroy and Y. Poullet 'The Right to Information Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in S. Gutwirth, P. De Hert and Y. Poullet, eds., *Reinventing Data Protection* (Springer, 2009) 45.
[111] See D.J. Solove and W. Hartzog 'The FTC and the New Common Law of Privacy (2014) 114 Columbia L Rev 583 ("in practice, FTC privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States — more so than nearly any privacy statute or any common law tort.")
[112] See *infra*, heading 5.3.

and data quality (data should be correct and up-to-date), purpose specification and use limitation (data may only be processed for previously specified purposes of original collection). The design of data-processing systems should be aimed at processing either no personal data at all or as few as possible (the principle of data avoidance, or data minimisation).[113] Under the principle of data security, the data controller bears a statutory obligation to ensure that personal data are processed in a secure environment preventing unauthorised destruction or access (Article 17 DPD).

All personal data may only be processed when one of the grounds of lawful processing under Article 7 DPD is present: free and informed consent given specifically in relation to the purpose of collection, contract, legal obligation of a data controller, vital interests of a data subject, task in public interest or official authority of a controller or a third party, or legitimate interest of a controller or a 3rd party.

Special categories of personal data are subject to a stricter regime (Article 8 DPD). They include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life. By default, processing of such data is prohibited, unless one of the lawful grounds of processing under Article 8(2) DPD is present: consent of the data subject which – in addition to free and specific – needs to be explicit, unless the ban on processing cannot be lifted by consent under national law; obligations and specific rights of the controller in the field of employment law, authorised by national law; protection of vital interests of the data subject or another person, where data subject is incapable of consent; when data is processed by non-for-profit organisations, in the course of their legitimate activities, regarding its members; or when data is manifestly made public by the data subject, or necessary for defence of a legal claim. In addition, health data may be processed for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, by a medical professional under obligation of professional secrecy (Art. 8(3) DPD).

Data transfers to non-EU countries are allowed only if such countries provide an 'adequate level of protection' as ascertained by the European Commission (Article 25 DPD).[114] By way of derogation, member states may allow data transfers to countries without an adequate level of protection under a restricted number of circumstances under Article 26 DPD (such as the data subject's consent, or when the controller adduces adequate safeguards, e.g. in the form of contract clauses or Binding Corporate Rules).

4.4.2. Implementation mechanisms

The substantive rules and principles of data protection are brought into effect by an implementation mechanism that combines the data subject's rights and the controller's obligations; judicial remedies, norms on liability and sanctions; and governance.

[113] B. Holznagel and M. Sonntag, 'A Case Study: The JANUS Project' in C. Nicoll et al., eds., *Digital Anonymity and the Law – Tensions and Dimensions* (The Hague: TMC Asser Press, 2003) 121.
[114] On this point, see ECJ, 6 October 2015, *Schrems* ECLI:EU:C:2015:650.

The data subject has a number of data protection rights: information rights (Articles 10 and 11); right to access personal data processed and request rectification, erasure and blocking in case of non-compliance with the Directive, backed by the data controller's obligation to notify third parties about such erasure requests (Article 12 DPD); right to object to data processing on compelling legitimate grounds (Article 14 DPD). In the *Google Spain* ruling,[115] the European Court of Justice interpreted Article 12 and 14 rights to include a right to request a search engine provider to delete links from search results when one's name is a search word. This right is often referred to as 'the right to be forgotten.' Each right is backed up and effectuated by a corresponding obligation on the part of the controller. In addition, the controller bears an obligation to notify national supervisory authorities and publicise data processing (Articles 18, 19, 21 DPD) and conduct 'prior checking' when processing presents specific risks (Article 20 DPD).

To enforce the data protection rights and obligations, the data subject, organisation or association may lodge a complaint with a national supervisory authority (Article 28 DPD); data subjects have a right to seek judicial remedy (Article 22 DPD) and receive compensation from the controller for damage suffered as a result of unlawful data processing (the controller is exempted from liability if it can prove not to be responsible for the damages) (Article 23 DPD). Member States may impose criminal, administrative or other sanctions for the data protection violations (Article 24 DPD).

Independent national data protection authorities (DPAs) are charged with monitoring the application of data protection law as implemented by national measures and are endowed with investigative powers, powers of intervention, and to engage in legal proceedings; hear complaints; cooperate with other DPAs; and carry out prior checking (Article 28 DPD).

The GDPR builds upon these implementation mechanisms, endowing national authorities with increased powers, including the explicit power to fine firms for non-compliance.

4.4.3. The DPD, harmonisation and divergences between Member States

While the DPD is an instrument of 'generally complete' harmonisation,[116] Member States retain leeway in how they interpret or clarify the principles of the DPD,[117] and in how they enforce the DPD. Since the DPD did not introduce a home-country control system – where only one Member State has jurisdiction for the entire activities of a firm throughout the EU – firms have no choice but to comply with up to 28 national laws as they do business across the EU.

The complete harmonisation of data protection laws only precludes Member States from adding additional elements to the harmonised provisions, e.g. new grounds of legitimate processing in

[115] ECJ (Grand Chamber), 13 May 2014, Case C-131/12, *Google Spain* ECLI:EU:C:2014:317, discussed above. This right to be forgotten is now included in the proposed GDPR.
[116] ECJ, 24 November 2011, Case C-468/10 *ASNEF* [2011] ECR I-12181 at para. 29 and Case C-101/01 *Lindqvist* [2003] ECR I-1297 at para. 96, 97.
[117] C. Millard and W.K. Hon 'Defining "Personal Data" in e-Social Science' (2011) 15 Information, Communication and Society 66.

addition to the ones listed in Art. 7, but still "leaves to the member states the task of deciding the details or choosing between options".[118] In so doing, Member States might take diverging routes. We provide two examples here: the very definition of 'personal data' itself and the application of the purpose limitation principle to further processing.

Definition of personal data

The concept of personal data is a key concept of the EU data protection regime and is one of the instances of divergent implementation of EU data protection law. 'Personal data' is a core concept of EU data protection, since as soon as the information processed constitutes personal data, this triggers the application of the data protection law. Information that is not personal data is outside of the scope of the DPD.

Briefly, the DPD defines personal data as any information that relates to an identified or identifiable natural person (Article 2 (a) DPD). The GDPR uses the same definition. This is a general definition that may be interpreted broadly or narrowly. Therefore, the practical implementation of that definition in the national laws is characterised by uncertainty and divergent national approaches[119] to issues such as when a natural person is identifiable. A non-binding interpretation by the Article 29 Working Group is the most inclusive,[120] whereas the implementation given to it in the UK Data Protection Act is one of the most restrictive.

The Article 29 Working Group understands the concept of identifiability in light of Recital 26 of the Data Protection Directive, meaning that "to determine whether a person is identifiable, account should be taken of *all the means* reasonably likely to be used either by the controller *or by any other person* to identify the said person" (emphasis added). This is the so-called absolute approach.[121]

The UK Data Protection Act focuses upon whether data is identifiable to the data controller as such, rather than to any other person.[122] This is the so-called relative approach, which marks a significant limitation on the scope of the Act as compared to the Directive. As a result, private parties may process the same data relating to individuals that counts as personal data in the Member States that follow the absolute approach, and as anonymous data under the UK law and the law of other jurisdictions that adopted the relative approach.

The jurisdictions that choose a narrow definition of personal data choose a narrow material scope of application of the data protection law and a lighter burden of compliance. This is because the data protection law and its principles, rules of processing and obligations only apply if 'personal data' is processed, and do not apply where the data processed is not 'personal'. The jurisdictions using a broader definition may be considered as imposing a heavier burden of compliance.

[118] V. Reding 'The European data protection framework for the twenty-first century' (2012) 2 International Data Privacy Law 121 and CJEU, Case C-468/10 *ASNEF, supra* note 115 at para. 35.
[119] Article 29 Working Party Opinion 4/2007 on the concept of personal data, WP 136 (20 June 2007) at 3.
[120] Millard and Hon, *supra* note 116.
[121] WP 136, *supra* note 118 at 15.
[122] M. Taylor *Genetic Data and the Law* (Cambridge: Cambridge University Press, 2012) at 140.

Further processing under the purpose limitation principle

The purpose limitation principle (Article 6(1)(b) DPD) is another example of an open norm and an opportunity for divergent national implementation of the harmonised data protection provisions. It requires that personal data must not be further processed in a way *incompatible* with the original purpose or purposes of collection. What is considered compatible may be interpreted differently. National implementations of this principle vary from a strict interpretation – involving a formal comparison of the initial purpose of collection with the purpose of subsequent use – to a more accommodating approach that allows a degree of flexibility. The Article 29 Working Party, in an attempt to achieve a common understanding of the purpose limitation principle, issued an opinion where it explains how the principle should be understood.[123] However, the opinion is not binding.

In addition to divergent implementation of the substantive rules and principles, as set out above, the national data protection practices of the Member States also differ significantly in terms of how the data protection law is enforced. Notably, the Data Protection Authorities, the watchdogs of the European data protection regime, have different powers, varying degrees of independence and different internal procedures and approaches to how they enforce. A recent example of these differences is how the data protection authority of Hessen and the Information Commissioner's Office in the UK reacted to the Safe Harbor decision. The former – in an on-line statement of 26 October[124] – suggested an immediate ban on data transfers to the US based solely on Safe Harbor, as well as temporary moratorium on approvals for Binding Corporate Rules ("BCRs") and "data export agreements." The latter still believes Safe Harbor can be saved,[125] and advises not to "rush to make changes at this stage."[126]

The enforcement record of a national DPA may certainly be a factor when an international player from outside the EU – such as Facebook or Google – is choosing a Member State in which to establish[127] its subsidiary, or locate equipment, and hence determine which national law applies to its data processing activities, [128] or when a multinational designates a 'lead DPA' to approve its Binding Corporate Rules.[129] At the same time, under the DPD, DPAs retain the ability to exert their jurisdiction over non-EU firms if there is a sufficient basis to do so, despite the choices made by such non-EU firms. This was the case recently when a Belgian court ruled in

[123] Article 29 Working Party Opinion 3/2013 on purpose limitation, WP 203 (2 April 2013).
[124] https://www.datenschutz.hessen.de/ft-europa.htm#entry4521
[125] https://iconewsblog.wordpress.com/2015/10/27/the-us-safe-harbor-breached-but-perhaps-not-destroyed/
[126] http://www.bbc.com/news/technology-34646146
[127] Within the meaning of EU law.
[128] Article 4(1)(a)(c) DPD. Many non-EU controllers chose Ireland or Luxembourg for that purpose.
[129] The Article 29 Working Party gives guidance as to what criteria a corporate group should take into account when justifying its choice of a lead DPA, but these are not formal criteria and the DPAs exercise their discretion when deciding if they are the most appropriate DPAs for the purpose (see Article 29 Working Party Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules", WP 107 (14 April 2005) at para. 2.

favour of the Belgian Privacy Commissioner and ordered Facebook to modify its practice of tracking non-members when they visit Facebook pages.[130]

Accordingly, in some circumstances, firms might 'vote with their feet' and – to the extent they can – try to position themselves to fall under a more favourable jurisdiction. This may give rise to pressures on Member States on the losing end of that process to move towards the level of implementation and enforcement of the 'winners', a phenomenon known as 'regulatory competition'.[131] Regulatory competition refers to a situation where (i) economic actors are mobile and have a choice between the law of a number of jurisdictions, (ii) these jurisdictions have the ability to select the law they desire, (iii) the choice of each jurisdiction does not create externalities for the others.[132] Under these conditions, depending on the model followed, either actors will concentrate around the jurisdictions that offer them the law they prefer,[133] or jurisdictions will compete to attract actors and will change their laws accordingly, until an optimal solution emerges.[134]

Within the EU, once substantive law is harmonised, the room for regulatory competition diminishes since the various jurisdictions lose much of their ability to fashion their substantive laws around different sets of preferences. Accordingly, the risk of a race to the bottom is diminished, if not outright averted.[135] At most, some watered-down form of regulatory competition can take place, via applicable substantive law remaining outside of the coordinated area, the interpretation of the law or its enforcement. Such regulatory competition has been witnessed in, for instance, corporate law[136] or content regulation.[137]

[130] Brussels Court of First Instance, *Debeuckelaere* v. *Facebook* (9 November 2015), available at www.privacycommission.be.
[131] See the discussion of regulatory competition in P. Larouche "Legal Emulation Between Regulatory Competition and Comparative Law", in P. Larouche and P. Cserne, eds., *National Legal Systems and Globalization – New Role, Continuing Relevance* (The Hague, TMC Asser Press, 2013) 247 at the references mentioned therein.
[132] See F. Easterbrook, "Antitrust and the Economics of Federalism" (1983) 26 J. Law Econ. 23 at 34-35.
[133] This is the original, static model set out by C.M. Tiebout, "A Pure Theory of Local Expenditures" (1956) 64 J Pol Econ 416.
[134] This is the revised, dynamic model of Easterbrook, *supra* note 131 and other law and economics scholars.
[135] Unless the harmonisation is maximal. Conversely, minimal harmonisation protects against a race to the bottom, but would allow a race to the top.
[136] See ECJ, Case C-212/97, *Centros* [1999] ECR I-1459 and its progeny.
[137] See Larouche, *supra* note 130.

5. Opening up EU data protection law

The European approach to a data protection regime described above is a public law approach. It is based on the substantive rules and principles of data protection introduced via top-down regulatory mechanisms; compliance with these substantive rules is monitored and enforced by a public authority (national DPAs), and backed up by criminal, administrative and other sanctions under the national laws of the EU Member States. It is also self-contained and autonomous: starting from fundamental rights, which are by nature very general principles, a complete legal edifice has been constructed, to a large extent on its own, with its own set of concepts and definitions, its own understanding and its own epistemic community. And indeed, it is perceptible that, while EU citizens and policymakers are broadly supportive of a fundamental rights approach to privacy and data protection, they are not equally informed and assertive when it comes to the application of the more detailed content of EU law in the area. To put it bluntly, EU privacy and data protection law suffers from a 'reality gap' or a disconnect, as discussed above.

5.1. Reality gap

The perceived distance or disconnect between EU privacy and data protection law arises from both substantive law and from its enforcement.

As far as substantive law is concerned, the technological and business developments sketched at the outset of this report[138] challenge the foundations of the law. The DPD is remarkable for its functionalist approach: it is not attached to any specific system of data collection and processing. The definitions of 'data subject', 'controller', 'processing', etc. are such that they can be applied in different technological environments, from the manual collection of data to be entered on mainframes, as was still the case in the 1990s, to the automated collection of data via connected devices, uploading to the cloud, as we see it now. Nevertheless, despite the best efforts of its visionary drafters, the DPD is now showing its limits: it is built around a model where data collection and processing are ancillary to a main business activity. For example, an early online retailer (like Amazon when it started) builds a database of its customers, to help manage its sales process and to improve its customer experience. In that context, it makes sense to work with a model where data processing is done for a specific purpose (typically a subset of the main business process, e.g. supporting retailing operations), which is known at the outset and communicated to the data subject (the customer).

In this century, however, data processing has moved from an ancillary business function to a core business, for a large number of firms, including some very large firms such as Google or Facebook. These firms are now moving to the next phase in the business use of data processing, commonly known as 'Big Data'. Big Data involves the storage of data and its mining with a view

[138] *Supra*, Heading 2.

to uncover correlations that were not suspected when the data was collected. A number of core principles of the DPD – purpose limitation, data minimisation, storage and to some extent accuracy as well – are not necessarily compatible with the kind of data operations covered by 'Big Data'. Reconciling Big Data with the DPD comes at the price of re-interpreting some of these core principles, or restricting the ambit of Big Data operations.[139]

Furthermore, the DPD considers personal data collection as a bilateral operation between the individual data subject and the firm collecting the data.[140] It does not fully account for 'Web 2.0' services – including social networks – where data is generated through the interaction between individuals, such that it becomes difficult, if not impossible, to fit the collection and processing of such personal data within the conceptual scheme of the DPD. For instance, in the context of a social network like Facebook, much of the personal data comes from friendship links, or likes/dislikes, which involve two or more data subjects and which are generated by the data subjects themselves, leading to difficulties in identifying the data subject and the data controller.

As far as enforcement is concerned, despite all the efforts of the Member States' DPAs, there are limits as to what can be achieved under the public enforcement scheme of the DPD. First of all, the amount of personal data, and the number of firms holding such data as controllers or processors, continues to increase at a dizzying rate. The resources available to the DPAs to monitor and intervene in these processes are not increasing at a corresponding rate; even if the political will was there to fund the growth of the DPAs accordingly, it is doubtful whether such growth could be realised in practice. In addition to the growth in personal data volumes and in the number of data controllers/processors, the technology used for data collection and processing is also evolving rapidly. DPAs are therefore outplayed on all fronts (without any malicious intention implied or required on the part of data controllers and processors).

Next to the shortage of resources, DPAs also experience jurisdictional difficulties. These difficulties cut both ways: in some cases, many DPAs can potentially exert jurisdiction over a data controller, and coordination issues can arise. In other cases, especially when it comes to smaller data controllers not originating from within the EU, it is difficult for any EU DPA to assert jurisdiction meaningfully over that controller.

The combination of substantive discrepancies and limitations in public enforcement leads to this perception that EU privacy and data protection law, however well designed, is not effectively enforced – or even not effectively enforceable – in day-to-day practice, as perceived by data subjects (users).

The presence of a disconnect does not imply that EU privacy and data protection law is fundamentally misguided, or that it should be replaced by a more self-regulatory approach, as in

[139] For instance through wide-ranging anonymisation or pseudonymisation of data.
[140] The 'data controller' as defined in the DPD or GDPR.

the US. Rather, this report argues that one way to close this gap[141] would be to rely more strongly on the incentives of firms and citizens and seek to harness them in the service of the widely-shared public policy objectives set out in the DPD (and to be continued in the GDPR). In other words, while there are limits to what can be achieved with top-down public enforcement, the potential for private actors to willingly contribute to the public policy objectives is not fully exploited. To that end, the economic analysis of privacy provides useful insights, and private law offers an instrumentarium. Next to the quality of legislative drafting, internal consistency and adequacy of the substantive principles of data protection to cope with the challenges of modern data processing, the success of the upcoming GDPR also depends on the ability of the EU and its Member States to rely more on private law mechanisms, such as liability and contract, in order to bolster the protection offered by the DPD (and the GDPR) through private enforcement and to harness market forces to encourage firms to voluntarily provide a level of privacy and data protection higher than provided for in the DPD (and GDPR).

5.2. EU privacy and data protection law as a baseline

Due to the fundamental rights status of privacy and data protection, both in the system of the Council of Europe and the EU, as well as in the national legal systems of the EU member States, the freedom of private parties is restricted. Data protection rules cannot be 'contracted around' freely, and data protection guarantees cannot be waived by the data subject on market conditions, e.g. in exchange for money, goods, or services. To be clear, the commercial exchange and even 'sale' of personal data are not banned under the current approach. However, the existing data protection guarantees – general principles of data protection and specific rules regarding lawful grounds of processing, rights of the data subject and other – function as constraints on possible transactions.[142]

For instance, an individual may choose to share his or her personal data on a social network or with marketing companies in return for 'free' access to that social network or a discount. However, the party acting as controller will still be under the obligation to ensure that there is a legal ground of processing (consent that is free and specific to a clearly stated purpose and is a genuine expression of a choice), that the processing will be executed to the minimum necessary to achieve the stated purpose and the data will be processed no longer than necessary, be protected against unauthorised access or destruction, etc. The fact that a commercial exchange took place or that the individual consented to processing will not invalidate the individual's rights in relation to that data, such as to request its deletion or object to its processing. 'Selling' personal data meaning 'transferring absolute rights in that data', e.g. to use it for an unlimited

[141] This is in addition to other proposals to improve data protection enforcement. For instance, the draft General Data Protection Regulation gives more powers to the Data Protection Authorities, including the power to sanction for violations or to employ technology to aid individuals in exercising their control rights (so-called privacy-enhancing technologies, or 'PETs', and transparency-enhancing technologies, or 'TETs').

[142] As pointed out *supra* in Heading 3.1, an economic analysis of incentives in contracting is still applicable in such a setting when it includes these limitations as constraints in the contracting problem.

number of purposes, including re-selling, or for perpetuity is also excluded by the current data protection law.[143]

5.2.1. The DPD as a baseline for private parties

Beyond that, the presence of harmonised EU law via the DPD therefore influences how private parties can act in the sense that it provides markers around which private activities can be organised. At a minimum, EU law provides for default rules, in case parties cannot agree or do not bother to agree on other rules.[144] As is known, default rules also provide a focal point by which to judge any other alternative rules: these rules will be perceived first and foremost as either less or more protective than the default rules.

Yet the DPD is much more than a set of default rules: many of its core substantive provisions are couched in imperative terms. The DPD then forms a baseline, the foundation of a framework for the protection of privacy and personal data, around which the actions of private parties must be articulated.

These core provisions were set out above under Heading 4.4., and they will briefly be recalled here.

Data collection and further processing must fit under one of the listed grounds of lawful processing of Article 7 DPD (Article 6 GDPR), including but not limited to informed consent, contract, public authority or legal obligation and legitimate interest. There cannot be any exception to this requirement: if the subject did not consent, or no other ground applies, then processing is not lawful.

Furthermore, regardless of the applicable ground of processing, the purpose specification and limitation principle applies: data collection and processing must be done for a specific and legitimate purpose determined before consent is obtained and processing starts (Article 6 DPD, Article 5 GDPR). The purpose limitation principle cannot really suffer any exceptions, since if no purpose is specified, the data collection and processing are unlawful.

Furthermore, irrespective of how that collection is justified, the data controller must comply with the rights of the data subject. The rights of the data subject are listed in the DPD. The data subject must be informed of the identity of the controller, the purposes for which data is processed and other relevant information (right to information).[145] The data subject has the right to access the personal data pertaining to him or her.[146] He or she can also object to processing.[147] He or she also has the right to confidentiality and security of personal data.[148] The

[143] Purtova, *supra* note 78.
[144] Rules alternative to the default data protection rules can only be agreed on if they provide for a higher level of protection.
[145] Art. 10-11 DPD (corresponding provisions in GDPR: Art. 11-14).
[146] Art. 12 DPD (corresponding provision in GDPR: Art. 15).
[147] Art. 14-15 DPD (corresponding provisions in GDPR: Art. 19-20).
[148] Art. 16-17 DPD (the GDPR replaces these by a more complex regime of data security).

proposed GDPR would add thereto a strengthened right to rectification[149] and to erasure (right 'to be forgotten')[150] and a right to data portability.[151] Here as well, whilst the precise outlines and modalities of such rights can be open to debate, no exception can be made to them. If they are not granted to the data subject, the data controller is not complying with the law.

Next to or on the edges of these core principles, there is room for interpretation, either due to incomplete harmonisation and flaws of legal drafting, or due to a deliberate choice of the legislature to build in a possibility of value judgements and account for the richness and complexity of real-life data processing situations, or a combination of both. In other words, around the baseline, certain elements of the directive allow for different interpretations, all of which are reasonable, although they differ in the level of protection that results.

5.2.2. The future of the baseline model under the GDPR

As mentioned above, there is room for some regulatory competition to take place under the DPD. The GDPR seeks to address that issue by limiting the scope for divergence amongst Member States: indeed it is a regulation that goes directly into Member State laws. The room for Member States to introduce divergences through their respective implementations would therefore be removed.

In principle, by the same token, the GDPR should have strengthened the baseline function of EU privacy and personal data law, by making EU law less amenable to divergences emanating from Member States.

Yet on the two issues mentioned above, the GDPR does not settle anything. As regards the definition of personal data, whereas the Commission proposal clearly went for the absolute approach, specifying that personal data related to persons "who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person",[152] both the EP and the Council have removed that phrase from the definition. As regards further processing, the GDPR could reduce the ambit for interpretation, since it would specify a series of elements to be taken into account when assessing the purpose of further processing.[153]

As with any legal text, complete clarity remains an elusive goal: some provisions will always leave room for interpretation, and sometimes that room will only become apparent later on, once the legislative text is confronted with unanticipated realities.

Yet so far, the legislative history of the GDPR reveals a widespread misconception about the meaning and implications of the choice of an EU regulation as the legislative instrument. Just because a regulation is directly applicable does not mean that it should be specified down to the

[149] Art. 16 GDPR.
[150] Art. 17 GDPR.
[151] Art. 18 GDPR.
[152] Article 4(1) of GDPR (Commission proposal).
[153] GDPR, Article 6(3a) (Council general approach).

last detail: as mentioned in the previous paragraph, it is impossible to anticipate every case and contingency. It seems as if every stakeholder – from Member States to industry groups and individual firms – is jumping on the bandwagon and trying to ensure that every eventuality is catered for. As a result, the text of the GDPR is becoming more elaborate with each iteration.

For instance, amongst the grounds of lawful processing listed at Article 6(1) GDPR, two grounds (compliance with a legal obligation, and performance of a task in the public interest or in the exercise of official authority) refer to other parts of the legal system. Of course, those other parts can emanate from EU law or Member State law. In the Council general approach, a long clause has been added (at Article 6(3)) to enable Member States to derogate in their legislation from most of the core provisions of the GDPR, thereby creating a large loophole for Member State law to undermine the level of protection guaranteed in the GDPR. In another vein, the principle of responsibility and accountability of the controller (Article 22 GDPR), which started out as a general statement,[154] has now been adorned with a long list of relevant factors, that does not make it any clearer or more predictable.[155]

Furthermore, whilst the possibility of 'forum-shopping' under the DPD was limited to non-EU firms, the GDPR tries to introduce a limited 'home-country control' system that would also benefit EU firms.[156] Accordingly, the range of firms that can engage in some form of forum-shopping could actually expand.

In the end, therefore, a more general DPD provision that was open to many interpretations will often be replaced by a more detailed GDPR provision, that in turn allows some leeway to Member States. Alternatively, that provision will include a number of refinements and exceptions that do not really improve its intelligibility. The quality of the law is not thereby improved; what is more, the baseline function of EU law, i.e. its ability to form a basic core around which parties can anchor their rights and obligations, is lost in the sea of detail.

Even if it might be too late in the legislative process to change much, we would recommend that the EU institutions, and the stakeholders, abandon any inaccurate view that an EU regulation must provide for every eventuality. Instead, they should simply accept that, as the GDPR is applied and as time passes and new realities arise, there will always be room to have reasonable disagreements on interpretation. They should concentrate on ensuring that the GDPR offers private parties a clear baseline of privacy and data protection, coupled with a degree of flexibility that allows the parties to negotiate, compete, and self-enforce privacy and data protection policies, as long as the baseline level of protection is not prejudiced.

[154] "The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation", in the Commission proposal.
[155] "Taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of risk for the rights and freedoms of individuals, the controller shall implement appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation", in the Council general approach.
[156] The Council general approach provides for a system where Member States retain their territorial competence, but one of the national supervisory authorities (that of the main establishment) takes a leading role in the supervision of transnational data flows: Articles 51 and 51a

In the end, what is really at stake with the GDPR is an opportunity to shift the room for interpretation away from the Member States and towards private parties. In other words, instead of the different interpretations being pursued uniformly but separately in respective Member States, they should ideally be observable in each Member State, around the baseline formed by EU law.

5.3. Incentives for private regulation within the DPD and GDPR

While there is room for private parties to influence personal data protection in the DPD (and in the GDPR), such private influence is typically conceived from a public law perspective, as a substitute to public regulation in the form of a set of co-regulation mechanisms, namely codes of conduct, certification and trust seals and – to some extent – binding corporate rules. We survey each of these in the following paragraphs.

5.3.1. Codes of conduct

Data controllers practise co-regulation and self-control collectively via national and European codes of conduct (which implement data protection principles within a specific industry), trust labels, and binding corporate rules. In contrast to the US, the European model of participatory implementation is not self-, but co-regulatory. The codes are based on the policy goals and principles given by public authorities and public bodies review and approve the proposed codes of conduct and binding corporate rules. On the other hand, neither is the model based purely on government regulation, as the controllers themselves draft the rules and standards that are specific to their industry.[157]

Article 27(1) DPD encourages the drawing up of industry codes of conduct to properly implement the data protection standards of the DPD in the specific context of individual industries and sectors. Examples of such codes of conduct are found in the financial services[158] and the public transportation sectors.[159] The DPD does not require a formal approval of such codes by public authorities. The codes can be adopted both at the national and European level and can be – if the code 'owners' so choose – approved by national data protection authorities ('DPAs') or the Article 29 Working Party, respectively.[160]

[157] Purtova, *supra* note 107 at 199. For more on the EU model of co-regulation and its comparison with the US model of self-regulation see D.D. Hirsch 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?' (2011) 34 Seattle U L Rev 439.

[158] E.g. Gedragscode voor de verwerking van persoonsgegevens van de Nederlandse Vereniging van Banken en het Verbond van Verzekeraars (Code of conduct of the Dutch Bank Association and the Union of Insurers regarding the processing of personal data) approved by the Dutch DPA on 13 April 2010.

[159] E.g. Gedragscode verwerking persoonsgegevens OV-chipkaart door OV-bedrijven (Code of conduct regarding processing by public transport companies of personal data in relation to public transport chip cards), the most recent available version of which was registered by the Court of the Hague on 13 February 2009, no. 16/2009

[160] A report to the Information Commissioner's Office names two European-wide codes of conduct: the International Air Transportation Association (IATA) and the Federation of European Direct and Interactive Marketing (FEDMA).

The GDPR builds upon the provisions of the DPD concerning codes of conduct, with the possibility to have a formal approval for them (from a data protection authority), a register of such codes, and provisions concerning compliance monitoring.[161]

5.3.2. Certification and trust seals

Trust marks, or privacy certification, are a form of self-regulation that is exercised without the participation of national and European supervisory authorities. They are issued by independent bodies to indicate compliance with relevant data protection rules and can be withdrawn in the case of violations.[162]

The DPD does not contain mandatory requirements regarding the standardisation or certification of products, processes or services. Groups of organisations can establish certification schemes (e.g. trust marks or seals of approval) based on self-imposed voluntary standards by means of codes of conduct, to certify that a provider/producer of an IT service/product complies with the requirements of the code. Such certification schemes are administered by the code of conduct 'owners' who are independent private entities, or national DPAs.[163] The latter issue data protection seals certifying compliance with local data protection law. The data protection authority of the German Land of Schleswig-Holstein (the 'ULD')[164] issues such a seal. The French DPA (CNIL) issues a similar data protection label[165]. On a European level, there is a European Privacy Seal ('EuroPriSe'),[166] a voluntary data protection certification scheme for IT products and IT-based services that comply with EU data protection laws, taking into account the national legislation of the Member States.[167]

The proposed GDPR incorporates that practice, encouraging the creation of certification mechanisms and data protection seals and marks, especially at EU level.[168] Certification is done by a supervisory authority or by a private certification body recognised for that purpose.[169] These certifications and seals can also be used to demonstrate that appropriate safeguards are in place for data transfers to third countries.[170]

[161] GDPR (Council general approach), Art. 38 and 38a. Note that the Council, in particular, has substantially expanded the provisions concerning codes of conduct.
[162] From a consumer's perspective, trust seals are a quality feature. Such a feature is observable before starting a contractual relationship with a private party collecting personal data.
[163] R. de Bruin et al., *Analysis and definition of common characteristics of trustmarks and web seals in the European Union*, Report (February 2005) at 38.
[164] https://www.datenschutzzentrum.de/faq/guetesiegel_engl.htm
[165] http://www.cnil.fr/la-cnil/labels-cnil/
[166] https://www.european-privacy-seal.eu/criteria/
[167] K. Bock, *Final Report*, EuroPriSe project, Deliverable R08, WP1
[168] GDPR, Art. 39 (common to all versions). In addition, Art. 39 GDPR in the EP 1st-reading version, next to recognising private seals, provides that any controller may request a DPA to certify that data processing is performed in compliance with the data protection legislation, by issuing the "European Data Protection Seal".
[169] GDPR, Art. 39 (2a) and 39a (Council common approach).
[170] GDPR, Art. 39 (1a) (Council common approach).

5.4. Making more room for private law mechanisms

The DPD leaves private parties some room to fashion their own privacy policies, and give them some force within the regulatory scheme, via codes of conduct or certification schemes. The GDPR expands upon that room, by adding trust seals and incorporating in legislation the possibility of adopting Binding Corporate Rules as a way to enable data transfers to third countries. At the same time, all of these possibilities conceive of the action of private actors within a co-regulation regime. Beyond the co-regulatory elements of the DPD and the GDPR, which fall within a public law approach, private law elements could be introduced into the scheme of the DPD and GDPR and given a greater role.

In particular, more attention should be paid to both the liability regime and the ability to contract for greater protection. In the model sketched out above, the DPD (and later the GDPR) form a baseline for the actions of private parties. Conduct falling below the baseline should lead to liability (5.4.1.), and conduct going above the baseline (i.e. giving more protection) should be encouraged (5.4.2.).

5.4.1. Private enforcement: Liability under EU data protection law

One of the main new features of the proposed GDPR is the increased level of responsibility of the data controller.

First of all, the principle of accountability, articulated by the Article 29 Working Party in its Opinion 3/2010 on the principle of accountability (WP 173),[171] and adopted both by the Commission Proposal and the Council text (Articles 5(f) and 22) imposes an obligation on the controller to *adopt* technical and organisational measures to ensure and *demonstrate* – in a transparent manner - that the data processing is consistent with data protection law.[172] Instead of relying on the data protection authority to approve its policies, the GDPR puts the onus on the firm itself to ensure compliance, and makes it accountable for it. While such a development should be welcome, EU institutions must, however, ensure that the firms are not caught between incompatible compliance requirements, arising from the proposed GDPR and from related instruments, such as the proposed Directive on data protection in criminal law[173] or the proposed Directive on Network and Information Security.[174] Data protection certification schemes provide the controller with an instrument to comply with the principle of accountability as 'such programs would contribute to prove that a data controller has fulfilled

[171] Art. 29 Working Party, 'Opinion 3/2010 on the principle of accountability', WP 173, 00062/10/EN
[172] That obligation is somewhat watered down, but not eliminated in the Council general approach, at Article 22.
[173] Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012)10 (25 January 2012), now also being discussed between the institutions.
[174] Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, COM(2013)48 (7 February 2013), now before the Council in 1st reading.

the provision; hence, that it has defined and implemented appropriate measures which have been periodically audited.'[175]

Secondly, by way of specification of the accountability principle, the data controller is required to implement Data Protection by Design and Data Protection by Default.[176] These two principles arise from practice and literature, and they are now picked up in the proposed GDPR. Data Protection by Design implies that the data controller takes privacy and data protection into account from the very start, when data processing activities are conceived, so that they are carried out in compliance with EU law. Data Protection by Default means that the data controller adopts default procedures that limit the processing of personal data to what is necessary for the legitimate purpose, and not more: this covers data collection, data processing as well as data storage.

With the increased level of responsibility of the data controller, one would expect a renewed attention on private enforcement via liability claims.

The DPD contains a provision on liability, at Article 23:

- Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.
- The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

In the GDPR, that provision is expanded upon, at Article 77:[177]

- Any person who has suffered material or immaterial damage as a result of a processing which is not in compliance with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.
- Any controller involved in the processing shall be liable for the damage caused by the processing which is not in compliance with this Regulation. A processor shall be liable for the damage caused by the processing only where it has not complied with obligations of this Regulation specifically directed to processors or acted outside or contrary to lawful instructions of the controller.
- A controller or the processor shall be exempted from liability in accordance with paragraph 2, if it proves that it is not in any way responsible**,** for the event giving rise to the damage.

The example of competition law shows that potential liability can have a powerful incentive effect on the behaviour of firms, since liability claims can exceed any form of public sanction

[175] WP173
[176] GDPR, Art. 23.
[177] This is the text of the Council general approach. In addition, 3 further paragraphs deal with joint and several liability as between two or more controllers or processors, and with court jurisdiction over claims.

(fine) imposed on the firm. Furthermore, damages awarded as a result of liability claims compensate the victims of breaches of competition law directly, thereby also giving them an incentive to be more active in policing firm behaviour. In the context of competition law, there are fears of frivolous or abusive claims, but these fears are linked to the relatively open nature of competition law provisions, which may be difficult and costly to apply.[178] In contrast, as long as the DPD (and the GDPR) provide a solid baseline, their breach can be relatively easier to ascertain than a breach of competition law.

Nevertheless, the experience with competition law in the past 15 years also demonstrates that liability claims give rise to a number of legal issues that must be solved before these claims can move forward. Many of these issues affect all or almost all claims (calculation of damage, standing, limitation, etc.), and they must be resolved before liability claims can become a real option for victims of breaches of competition law. In competition law, the Commission has chosen to move ahead with a Directive to address those issues,[179] instead of letting these issues be sorted out as claims are made, in the bottom-up fashion suggested by the ECJ.[180]

Seen in that light, the provisions of the DPD and the GDPR, whilst they do set out the basics of a liability regime, remain underdeveloped.[181] The DPD being a directive, missing and complementary elements will naturally be found in the laws of the Member States. With the passage to a regulation in the GDPR, the link with the national laws of the Member States is weakened. Accordingly, some further details might be added to the GDPR; alternatively, one can wait for case-law to arise and propose legislation to correct resulting problems, if any. However, the underdevelopment of the regime could also put a brake on the build-up of case-law, if it causes parties to choose not to file liability claims.

A first element in need of greater specification is the basis for liability. In this respect, it seems that two distinct situations are covered by the above provisions. Liability can arise because either (i) the controller has not lived up to the standards of the DPD (or GDPR) in the design of its operations or (ii) the controller complied with the provisions of the DPD (or GDPR), but in practice a security breach has occurred and personal data has been compromised.[182] In the first case, the breach arises at the decision-making level: the controller did not put in place an adequate data protection and privacy policy. In the second case, the breach is more operational in nature: despite having put adequate policies in place, security was still compromised during operations.

The distinction has implications for defences; the DPD (and GDPR) allow the controller to argue that it is not responsible for the event giving rise to the damage. In the first scenario, it is

[178] All the more following the move towards a greater use of economic analysis in the application of competition law.
[179] Directive 2014/104 of 26 November 2014 [2014] OJ L 349/1.
[180] In cases such as Case C-453/99, *Courage* [2001] ECR I-6297 and Case C-295/04 *Manfredi* [2006] ECR I-6619.
[181] In that sense, one should be mindful of the US experience with 'privacy torts'; they are widely criticised as being inadequate to address privacy violations as the damages from an individual violation of privacy are often hard to observe, let alone prove in court to the requisite standard.
[182] That second scenario can also be construed as a breach of the obligation to guarantee data security, bringing it in line with the first scenario, but that would not do justice to the differences between the two scenarios.

difficult to see how this defence can work: after all, the breach is in the design of the controller's policies, which do not comply with the DPD (or GDPR). The defence could prove useless in that scenario.

In the second scenario, however, the controller will try to show that the operational failure (breach of data security) came from the actions of a third party (hackers) and not its own. It is conceivable that such defence will often be successful; accordingly, the question would arise whether this defence is not too easily available. Already, the GDPR tightens the defence by adding the words "in any way" to the provision. Nevertheless, at the end of the day, the DPD and the GDPR create little more than a basic fault-based regime for privacy and data protection breaches, with a reversed burden of proof. This remains a modest achievement, compared to what was done for product liability[183] (a risk-based regime) or even competition law[184] (a regime with rebuttable presumptions). *De lege ferenda*, considering the principle of accountability now introduced with the GDPR, whereby the controller must take appropriate measures with a view to the risks involved in data processing, liability for security breaches could be risk-based, in line with product liability.

Next to this fundamental question, the DPD (and GDPR) remain silent on a number of other key issues for a liability regime to work: causation, limitation, recoverable damage, to name but the main ones. On that latter issue, there is some variation amongst Member States, which could justify further specification at EU level. In some Member States, the mere violation of privacy and personal data protection is held to constitute recoverable damage,[185] whereas in others, the victim must prove concrete harm (loss of reputation, financial loss, etc.) before the defendant can be made liable.

Beyond that, it seems that collective redress mechanisms would be needed for the regime to be fully effective, given that many breaches of privacy and data protection law touch a large number of victims, their negative effect is often cumulative and not individual, and the amount of damages to be expected (much of it being for non-material damage) is not always high enough to warrant incurring the costs of litigation.

5.4.2. Market mechanisms for a greater level of protection

Next to private enforcement for conduct falling short of the baseline set out in EU law, there is also a distinct possibility that private parties freely choose a higher level of protection than the baseline, possibly triggering a 'race-to-the-top', as the examples below illustrate.

[183] Directive 85/374 of 25 July 1985 concerning liability for defective products [1985] OJ L 210/29.
[184] Directive 2014/104, *supra* note 178.
[185] See for instance the case-law under Article 9 of the French *Code civil*.

Hierarchy between grounds of processing

Personal data may only be processed on one of the grounds of processing listed under Article 7,[186] including among others, consent of the data subject, a contract to which the data subject is (or will be) party, legitimate interests of the controller or third parties, etc.

All grounds of processing are considered equal, in the sense that there is no hierarchy or normative priority among them, and the controller is free to choose any ground that suits its purposes best.[187] Accordingly, the data controller could choose to give normative priority to consent, and only process personal data when free and informed consent is present.

At the same time, consent must always be valid. To be valid, consent must be freely given, specific (among others, to the particular purpose of processing) and informed (Article 2(h) DPD).[188] In some contexts consent is difficult to achieve, and other grounds of legitimate processing must be relied on instead. For instance, the data protection authorities advise against data processing based solely on grounds of consent in the field of electronic commerce, employment relationships,[189] electronic health records,[190] and data transfers outside the European Union. Many data protection authorities do not recognise consent given by a minor or a child.[191] These contexts may create a risk of forced or ill-informed consent.[192] In the context of e-commerce there is an increased risk that a data subject did not fully understand, or did not read, lengthy or unclear standard terms and conditions. Many data protection authorities also rightly see employment relationships as being inherently dependent, meaning that employees cannot meaningfully provide consent.[193]

Compelling legitimate grounds to object to data processing

Under Article 14 DPD, a data subject has a right to object "at any time on *compelling legitimate grounds* relating to his particular situation" to his/her data being processed, at least when the

[186] Or one of the grounds of the more limitative list of Article 8 for the special categories of personal data.
[187] The situation is not changed by the GDPR.
[188] This provision could be kept unchanged in the GDPR, should the Council general approach prevail over the proposal of the Commission (which would add that the consent must be explicit).
[189] 'The Article 29 Working group has taken the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data, it is misleading if it seeks to legitimize this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment.' (Article 29 Working Party Opinion on the processing of personal data in the employment context, WP 48 (13 September 2001) at 3.
[190] Article 29 Working Party Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131 (2007).
[191] C. Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford: OUP, 2007) at 211.
[192] *Ibid*. at 68
[193] Article 29 Working Party, *supra* note 188 at 3, stating '[t]he Article 29 Working group has taken the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is misleading if it seeks to legitimize this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment' (cited in ibid., pp. 211–212). See also *Nikon v. Onof*, decision No. 4164 (2 October 2001), in which the French Cour de Cassation did not allow the reading of an employee's email messages, even with the employee's consent (cited in Kuner, *supra* note 190 at 212).

processing is done on the grounds of legitimate interest (Article 7 (f) DPD) or performance of a task carried out in the public interest or official authority (Article 7 (e) DPD), save where otherwise provided by national legislation. The controller may no longer process these data where there is a justified objection. References to *compelling legitimate grounds* allow an entity acting as a controller to make a value judgment regarding whether the ground for objection is legitimate and compelling.

In the GDPR, the burden of this provision is reversed, with the controller having to demonstrate compelling legitimate grounds to override the objection of the data subject.[194]

Here the controller could decide to commit to stop data processing and erase personal data upon request of a data subject, i.e. to presume that any and all grounds for objection are compelling and legitimate, and therefore all objections justified.

Similarly, as regards the definition of personal data, discussed above, a controller could freely decide to opt for a more inclusive definition of personal data, in line with the interpretation adopted by the Article 29 Working Party (and as opposed to the UK interpretation).

It is not difficult to imagine that firms would choose to offer superior privacy and personal data protection. First of all, as was shown earlier,[195] under certain assumptions it is sensible for firms to commit to respect privacy and protect personal data, in order to foster the disclosure of information by consumers. Secondly, in a competitive market where network effects (one- and two-sided) confer a significant advantage to the leading provider, other competitors can try to gain an edge on the market by offering a higher level of privacy and personal data protection than the leading provider (on the assumption that there is demand for this).

Given that in the EU privacy and data protection are generally held to be desirable, this report encourages policy makers to revise policy with respect to privacy so as to harness consumer demand and the willingness of some suppliers to meet that demand, in order to give incentives to market actors to opt for more protection, and thereby to give momentum to a scenario that, at least in some markets, gives rise to a 'race to the top'.

Furthermore, one of the main objectives of the proposed GDPR is to better reconcile data protection and innovation. Seen in that light, the GDPR should offer a sustainable framework for firms to offer innovative privacy and personal data protection as part of their innovative services. The principles of Data Protection by Design and Data Protection by Default, as set out earlier, aim precisely at ensuring that firms take data protection seriously from the very start when they seek to bring innovative products to the market. Other elements in the DPD and the proposed GDPR, in contrast, are often said to create a rather static framework that is not conducive to innovation. One example of such provision is the purpose limitation principle. As set out earlier,[196] new and innovative data processing technologies – the so-called 'Big Data' – involve an element of uncertainty that cannot easily be reconciled with the purpose limitation

[194] GDPR, Article 19 (no significant differences between the institutions on this point).
[195] Heading 3.4.1. above.
[196] Heading 2. above

principle. Unless the controller states the purpose of personal data processing very vaguely and broadly,[197] possible new uses of personal data will come up in the course of 'Big Data' processing, that are not covered by any statement of purpose.

In the current discussions surrounding the proposed GDPR, 'anonymisation' is put forward as a technical solution to that issue, by which personal data can be 'anonymised' through irreversibly stripping personal data of identifiers that could link these data to a natural person, and thereby taken out of the scope of the GDPR. However, the possibility of true anonymisation is currently questioned, since advances in Big Data analytics – in terms of amounts and variety of data available for analysis, and of sophisticated algorithms – effectively make true and irreversible anonymisation unattainable.[198] The GDPR provides for another variety of data – "pseudonymous data", i.e. personal data which has gone through the process of pseudonymisation, after which "the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution".[199] However, pseudonymous data remains personal data within the meaning of the GDPR, and hence must be processed in compliance with the rules and principles of the GDPR, including purpose limitation.

Because Big Data is said to carry significant social benefits, some scholars argue that the principles of privacy and data protection, such as purpose limitation, "must be balanced against additional societal values such as public health, national security and law enforcement, environmental protection, and economic efficiency."[200] Tene and Polonetsky propose to rest a new data protection framework on a risk matrix, "taking into account the value of different uses of data against the potential risks to individual autonomy and privacy."[201] Schwartz and Solove propose to introduce a granular concept of personal data, based on the risk of causing privacy harms related to the likelihood of identification, where personal data is subject to different legal regimes depending on the risks.[202] At the same time, adopting a risk-based approach to data protection and leaving aside or downplaying substantive principles of data protection has downsides as well, including the lack of clear understanding of the harm that new technologies such as Big Data analytics could cause, or the danger that data protection compliance will turn into an exercise of managing reputational and liability risks, rather than the risks of data processing.[203]

[197] Which would turn the purpose limitation principle into an empty shell and might not be compatible with it. In contrast, the approach proposed above attempts to preserve the purpose limitation principle as a meaningful part of personal data protection.
[198] E.g. P. Ohm 'Broken Promises of Privacy' (2010) 57 UCLA L Rev 1701 at 1742 et seq. and 1759; A. Narayanan and V. Shmatikov 'De-anonymizing Social Networks' (2009) Publications of 30th IEEE Symposium on Security and Privacy 173, available online at <http://ieeexplore.ieee.org>
[199] GDPR, Article 3b, Council general approach.
[200] O. Tene and J. Polonetsky 'Privacy in the age of Big Data' (2012) 64 Stan L Rev Online 63.
[201] Ibid.
[202] P. Schwartz and D.J. Solove 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 NYU L Rev 1814.
[203] E.g. R. Gellert 'Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative' (2015) 5 International Data Privacy Law 3.

While innovation – through Big Data or otherwise – may be hampered by the principle of purpose limitation, the principle should not necessarily be abandoned on that account alone. Indeed, purpose limitation facilitates individual control over data processing, which remains a cornerstone of European data protection.

For one, the principle of purpose imitation under the DPD and GDPR already accounts for the possible public benefits of data processing. The GDPR does not rule out further processing of personal data for purposes other than the original purpose of collection, when further processing is done "for archiving purposes in the public interest or *scientific*, statistical or historical purposes".[204] Big Data does not always automatically serve innovation and the public good: even scientific uses, explicitly listed as exceptions to the purpose limitation principle, may appear unethical, contrary to public interest or otherwise socially undesirable.[205] Hence, if the application of purpose limitation, or for that matter any other data protection principle, should be relaxed in part, this should not be done uniformly across the board, and without introducing any additional safeguards. Such a possibility is not addressed in the GDPR, and the research on these issues is still at an embryonic stage.

As another alternative, one could think of encouraging a more fluid system of purpose limitation, whereby the purpose of personal data processing would not be fixed at a specific point in time but could be revised and adapted in tune with advances in 'Big Data' processing. In return, the data subject would also have to be more closely involved in the management of his or her data, through constant information, coupled with the opportunity to confirm consent or object to further processing. Such a fluid system can probably be carried out already on the basis of the proposed GDPR. Nonetheless, it would be helpful if the GDPR provided more expressly for the possibility of a continuing relationship between data subject and controller, as opposed to the snapshot, static view now embodied in the purpose limitation principle. Such a continuing dialogue on privacy and personal data protection, in the context of innovative uses for data, would create room for the baseline of EU law to be implemented in an evolutive fashion, in step with innovation and with the principles of Data Protection by Design and by Default.

Realistically, individuals are unlikely to negotiate on privacy and data protection one-on-one with firms. In our daily lives, we accept standard contractual clauses – including privacy policies – on a routine basis as we make use of online services. Accordingly, if there is any potential for a 'race to the top', a move towards greater protection of privacy and personal data via the operation of markets, it will be realised through the privacy policies found in standard terms of contract, or in the best case scenario, through favourable privacy conditions placed as a core feature of a fixed offering (tariff, plan, etc.).

[204] GDPR, Art. 5(1).
[205] By way of example of a scientific study that allegedly breached ethical guidelines, although it does not involve Big data, a Facebook experiment involved Facebook users without their informed consent, where the researchers manipulated the content of newsfeeds to study their effect on mood (reported in http://www.theguardian.com/technology/2014/jun/30/facebook-emotion-study-breached-ethical-guidelines-researchers-say)

With its provisions on codes of conduct, the DPD already makes room for private initiatives to grant further-reaching protection. The GDPR goes further by codifying the practice on certification and trust marks, as well as BCRs. Yet as mentioned above, the approach of the DPD – continued under the GDPR – fits a co-regulation model, and is inspired by public law.

If the aim is to provide incentives for firms to offer more than the baseline of the DPD (or GDPR), more is required than just creating room for co-regulatory mechanisms. We cover here three important prerequisites for a 'race-to-the-top' to occur. First of all, consumers must be able to move from one firm to the other, hence the principle of data portability. Secondly, competition among firms to offer a higher level of privacy and personal data protection must be fostered and protected. Thirdly, and perhaps more fundamentally, moral hazard and adverse selection problems must be addressed, lest they lead to market failure.

The proposed GDPR enshrines a right to data portability, at Article 18. Data portability comprises, first of all, the right to receive personal data from the controller, in a structured and commonly used machine-readable format and, secondly, the right to transmit the personal data to another controller without hindrance from the first controller.[206] Data portability has been hailed as one of the main innovations in the GDPR, and indeed it is essential in order for consumers to be able to change providers. At this point in time, not all controllers offer data portability, and as a result some consumers are locked into their choice of provider. In the era of data-centric business models and user-generated content, the amount of personal data generated and stored by a firm offering social network services, for instance, can be such that a consumer cannot face the prospect of losing that data if he or she were to move to another firm. Beyond that, the principle of data portability could also have an influence on innovation, by creating a need for standardisation of data format (*de facto* or via a standard-setting organisation). Whilst it is almost indispensable for portability to work, standardisation also fixes some formats, interfaces or protocols, and it therefore has an impact on the flow of innovation.

The right to data portability envisaged in the GDPR might not be enough to make markets work, however. The personal data of individuals (data subjects) is of course useful for any provider to hold and use, but beyond that it is often the ability to aggregate personal data which makes leading providers so powerful. For instance, search engine providers can fine-tune the results offered to a user not just in the light of the personal data they hold over that user, but also in the light of the aggregate personal data of other users: the search engine will know what users with similar personal characteristics were looking for when they introduced specific search queries, and will use that knowledge to improve upon the performance of the search engine. That aggregate knowledge, where network effects have been argued to play a role, is hard to port.

Secondly, once data portability is seen not just as a right of the data subject, but as a prerequisite for competition to function, then that competition must be protected, where necessary, through the application of competition law. As shown above in the overview of the

[206] Provided the processing is based on consent or a contract, and it is done by automated means.

economics of privacy and data protection, personal data can play a role in competitive outcomes. Here the emphasis would be primarily on the prohibition on abuses of dominant position, at Article 102 TFEU. For instance, if a dominant firm breaches the right to data portability and prevents its users from taking their personal data to another firm, then there could also be an abuse within the meaning of Article 102 TFEU.[207] By the same token, if a dominant firm breaches personal data protection legislation in such a way that the firm obtains personal data unlawfully and uses it to gain a competitive advantage over its rivals, then liability under Article 102 TFEU could complement private law liability towards the data subjects, as outlined earlier. More speculatively, as suggested in the previous paragraph, a dominant firm might conceivably be forced to give access to the aggregate of the personal data itself (beyond portability), should that data qualify as some form of essential facility.[208] Next to Article 102 TFEU, it also possible to envisage a role for Article 101 TFEU – in the case of agreements between firms concerning the exchange of personal data, for instance, which would restrict competition by foreclosing others[209] – or the Merger Control Regulation – should a merger bring the merging firms to a position to behave anti-competitively because of their position as regards personal data.[210] The cooperation required among firms in order to create and implement codes of conduct or certification schemes also raises potential issues under Article 101 TFEU. So far, however, EU competition authorities have proven reluctant to incorporate personal data protection concerns in their analysis.

Finally, even if users can port their data from one firm to the other, and even if competition over or via privacy and personal data is policed, there remains a risk of market failure through moral hazard or adverse selection. As a starting point, considering the economics of privacy, as set out above in section 3, if firms offer greater protection of privacy and personal data, they are often less able to derive value from personal data. The associated loss would have to be offset somehow to make firms willing to engage in greater protection; customers could be requested to pay something to enjoy stronger privacy protection (as opposed to enjoying 'free' services), or bear with inferior performance (due to increased protection). This commercial proposition crucially depends on whether customers believe that they will be obtaining superior privacy and personal data protection. If customers correctly do not believe the superior privacy claims made by firms, firms do not have an incentive to offer privacy protection, a situation referred to as moral hazard.

Alternatively, if this provision is beyond the control of firms, but firms' offerings have inherently different privacy propositions, those firms with stronger protection may not survive in a market,

[207] Indeed hindering data portability is one of the allegations leveled at Google on both sides of the Atlantic. Google would have prevented advertisers from taking their data (advertising campaigns, formatted to be served on Google's advertising platform) to competing online advertising platforms.
[208] See the suggestion made by C. Argenton and J. Prüfer 'Search Engine Competition with Network Externalities' (2012) 8 J Comp Law Econ 73.
[209] In Case C-235/05, *ASNEF*, *supra* note 115, the ECJ found that data protection concerns should not enter into Article 101 TFEU analysis.
[210] The Commission refused to entertain these arguments, on a formalistic ground that data protection does not factor into competition law analysis, in *Google/Double Click* [2008] OJ C 184/10.

leading to adverse selection (Akerlof, 1970). In such an environment claims to superior quality are not credible, as such offers are not profitable when consumers assume that all products have inferior quality. This is compatible with consumers refusing to pay a premium price as they correctly foresee that products of superior quality will not be available. This argument applies to privacy and personal data. If customers find that firms are not credible when they claim to offer superior privacy and personal data protection, then they will refuse to use the offerings of those firms, let alone purchase them; over time, the market will settle the minimum level of protection. In such a case, few offerings may be available and, in the extreme, the market completely breaks down.

To provide incentives for private parties with superior quality to stay in the market (and possibly to choose stronger privacy protection), data protection authorities must ensure that consumers accept and trust codes of conduct, certification and trust marks. Their role should therefore go beyond merely testing whether these private instruments comply with the DPD (or GDPR), and also encompass advocacy in favour of instruments that provide a higher degree of protection. One could think, for instance, of a trust mark with many levels, from 1 (basic, meets the requirements of the GDPR) to 5, expressed in stars, as is customary for seller ratings in electronic commerce. Data protection authorities should then not only accept the use of trust marks, but also (while policing compliance) encourage their acceptance and contribute to their trustworthiness.

An important issue in this context is who controls a trust mark. While the market may provide it in the absence of an active data protection authority (Biglaiser, 1993), there is a risk that the market does not provide a trust mark efficiently. In particular, a private party controlling a trust mark may not have an incentive to increase the information available to consumers about the privacy policy offered by firms.[211] Then the optimal governance of trust marks would require some direct involvement of a data protection agency or some other public body.

[211] This argument is formalised by A. Lizzeri 'Information Revelation and Certification Intermediaries' (1999) 30 RAND Journal of Economics 214 in the context of adverse selection and G.L. Albano and A. Lizzeri 'Strategic Certification and Provision of Quality' (2011) 42 International Economic Review 267 in the context of moral hazard.

6. Conclusions and policy recommendations

While privacy issues affect network industries as they affect other sectors of the economy, firms in network industries are often subject to additional rules concerning privacy and personal data protection, in the forms of sector-specific privacy legislation or specific privacy provisions in sector-specific regulation. These additional rules are often not aligned with the general standards of the DPD (and the proposed GDPR), thereby distorting competition with other firms that are not subject to such specific legislation. We therefore recommend that sector-specific privacy legislation – in particular the ePrivacy directive – be closely reviewed and, if possible, repealed.

We also recommend that law and policymakers pay closer attention to the expanding economic literature on privacy and data protection. The literature shows that the welfare effects of privacy and data protection regulation are not unambiguous, and that accordingly a differentiated and nuanced approach is required. Intervention could be warranted, however, to correct the 'privacy paradox' whereby individuals do not act in line with their stated preferences as regards privacy.

In response to the 'reality gap' affecting EU privacy and personal data protection law, we do not recommend reverting to a self-regulatory approach on the US model. Rather, we recommend casting the DPD (and the proposed GDPR) as a baseline, around which the actions of private parties can be organised. For that purpose, we recommend that the proposed GDPR, instead of precisely mapping exceptions and remaining areas for Member State laws, should focus on setting out the basic principles, so as to guide private parties.

In particular, we recommend that the GDPR make more room for private mechanisms of compliance and enforcement, in addition to the codes of conduct, certification and trust marks that are already provided for.

First of all, for conduct falling below the baseline of the GDPR, private enforcement via liability claims should be encouraged. We recommend that the EU institutions ensure that the accountability of the data controller is not affected by divergences between the GDPR and related legislation such as the proposed directives on Personal Data Protection in Criminal Matters, and on Network and Information Security. The liability regime of the GDPR should be further developed and specified, using precedents in EU law (product liability, private enforcement of competition law) as an example.

Secondly, private incentives to offer a greater degree of protection than under the baseline of EU law should be encouraged. The GDPR already introduces the right to data portability, but more portability might be required. Indeed, we recommend that EU competition law be developed to better incorporate privacy considerations in the analysis, especially under Article 102 TFEU. Finally, we recommend that EU and national authorities advocate pro-actively in favour of certification schemes and trust marks, in order to avoid moral hazard or adverse

selection problems ('market for lemons') that could arise if firms that want to offer better protection cannot credibly convey their proposition to their customers.

Postscript

In December 2015, as this project was concluded, the EU institutions agreed on a compromise text for the General Data Protection Regulation. The compromise text does not differ from the negotiating texts available at the time of writing to such an extent as to affect the analysis conducted in this report. The following points can be noted, however.

In line with the fears expressed in this report, the compromise text is muddied: for each statement of principle, one finds reservations or exceptions immediately attached. This undermines the clarity and legibility of the GDPR, and will make it more difficult for the GDPR to fulfill its baseline function. Accordingly, at a time where the future of data protection law in Europe requires that private actors play a greater role in the enforcement and development of the law, the GDPR makes the tasks of private actors more arduous by giving them a very complex legal framework to work with. While EU institutions sought to provide for every eventuality in the GDPR, on the misguided ground that it is an EU regulation, they might in the end have created more room for interpretation and litigation than there was before under the DPD.

When compared with the negotiating texts used in preparing this report, as regards further processing, the compromise text leaves the possibility to rely on consent to extend the processing to another purpose.[212] In the absence of consent, the controller retains the ability to find that further processing is compatible with the original purpose, in the light of a list of criteria. That list now explicitly mentions encryption and pseudonymisation as appropriate safeguards for further processing, opening the door to the use of these two techniques in the course of further processing (data mining and Big Data analysis).

Furthermore, as regards the right to data portability, the compromise text has added a right to obtain that the data to be ported is transmitted directly from one controller to the next, where technically feasible.[213]

Finally, another relevant addition in the compromise text, concerns the review of other EU personal data protection instruments, including the ePrivacy Directive. The Commission is now expected to submit legislative proposals to that effect, if appropriate.[214]

In the end, as this report anticipated, the main challenge for personal data protection, in the context of network industries and beyond, will be to live up to the promise of the legislative exercise that resulted in the GDPR, namely less fragmentation in the law across the EU. The compromise text, despite its level of detail, is bound to require considerable interpretation and coordination efforts if it is to lead to more uniformity in the law. In addition, the reality gap

[212] Article 6(3a). The text also provides that controllers can invoke EU or Member State law concerning central public policy aims (as listed at Article 21(1)) to justify further processing for another purpose than the original purpose of collection.
[213] Article 18.
[214] Article 90a.

identified in this report needs to be closed. This is why the involvement of private actors, along the lines outlined in this report, will prove crucial to the future of privacy and personal data protection in the EU.

References

Albano, G.L. and Lizzeri, A. (2001), Strategic Certification and Provision of Quality, International Economic Review, 42: 267-283.

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In: Proceedings of the 5th ACM Conference on Electronic Commerce, pp. 21-29.

Acquisti, A., Brandimarte, L., and G. Loewenstein (2015). Privacy and human behavior in the age of information. Science 347, 509-514.

Acquisti, A. and R. Gross (2006). Imagined communities: Awareness, information sharing, and privacy on Facebook. In: Danezis, G. and P. Golle (eds.). Privacy enhancing technologies. Springer.

Acquisti, A., L. K. John, and G. Loewenstein (2013). What is privacy worth? Journal of Legal Studies 42, 249-274.

Acquisti, A., C. R. Taylor and L. Wagman (2015). The economics of privacy. Forthcoming in Journal of Economic Literature.

Acquisti, A. and H. R. Varian (2005). Conditioning prices on purchase history. Marketing Science 24, 367-381.

Anand, B. and R. Shachar (2009). Targeted advertising as a signal. Quantitative Marketing and Economics 7, 237-266.

Argenton, C. and J. Prüfer (2012). 'Search Engine Competition with Network Externalities' 8 J Comp Law Econ 73-105.

Belleflamme, P. and M. Peitz (2015). *Industrial organization: Markets and strategies*. 2nd edition. Cambridge, UK: Cambridge University Press.

Bergelson, V. (2003). 'It's Personal, but Is It Mine? Toward Property Rights in Personal Information' 37 UC Davis L Rev 379-451.

Biglaiser, G. (1993), Middlemen as Experts, RAND Journal of Economics, 24: 212-223.

Bignami, F. (2007). 'The U.S. Privacy Act in Comparative Perspective', Contribution to the EP Public Seminar 'PNR/SWIFT/Safe Harbour: Are Transatlantic Data Protected?'.

Brandimarte, L. and A. Acquisti (2012). The economics of privacy. In: Peitz, M. and J. Waldfogel (eds.). The Oxford handbook of the digital economy. Oxford: Oxford University Press.

de Bruin, R. et al., (2005). *Analysis and definition of common characteristics of trustmarks and web seals in the European Union*, Report.

Byford, K.S. (1998). 'Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment' 24 Rutgers Computer & Tech. L.J. 1-72.

Campbell, J. D., A. Goldfarb, and C. Tucker (2015). Privacy regulation and market structure. Forthcoming, Journal of Economics & Management Strategy.

CERRE (2014). *Regulating Smart Metering in Europe: Technological, Economic and Legal Challenges*, available at www.cerre.eu.

Chemerinsky, E. (1999). 'Substantive Due Process' 15 Touro L Rev 1501-1534.

Cohen, J. (2013). 'What privacy is for' 126 Harvard L Rev 1904-1933.

Easterbrook, F. (1983). 'Antitrust and the Economics of Federalism' 26 J. Law Econ. 23-50.

Farrell, J. (2012). Can privacy be just another good. Journal on Telecommunications & High Technology Law 10, 251.

Fudenberg, D. and J. Tirole (2000). Customer Poaching and Brand Switching. Rand Journal of Economics 31, 634-657.

Fudenberg, D. and M. Villas-Boas (2006). Behavior-based price discrimination and customer recognition. In: T. Hendershott (ed.). Handbooks in information systems: Economics and information systems. Amsterdam: Elsevier.

Gellert, R. (2015). 'Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative' 5 International Data Privacy Law 3-19.

Goldfarb, A. and C. Tucker (2011). Privacy regulation and online advertising. Management Science 57, 57-71.

Goldfarb, A. and C. Tucker (2012). Shifts in privacy concerns. American Economic Review (Papers and Proceedings) 102, 349-53.

Gormley, K. (1992). 'One hundred years of privacy' Wisconsin L. Rev. 1335-1440.

Hermalin, B. and M. Katz (2006). Privacy, property rights and efficiency: The economics of privacy as secrecy. Quantitative Marketing and Economics 4, 209-239.

De Hert, P. (2003). "Making Sense of Privacy and Data Protection: A Prospective Overview in the Light of the Future of Identity, Location-Based Services and Virtual Residence" Annex I in Institute for Prospective Technological Studies, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview* (Report EUR 20823 EN).

Harris, D.J. et al. (2009). *Harris, O'Boyle & Warbrick Law of the European Convention on Human Rights*, 2nd ed (Oxford University Press).

Hirsch, D.D. (2011). 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?' 34 Seattle U L Rev 439.

Hirshleifer, J. (1971). The private and social value of information and the reward to inventive activity. American Economic Review 61, 561-574.

Hoeren, T. & A. Rodenhausen (2008). 'Constitutional Rights and New Technologies in Germany' in R. Leenes, B.-J. Koops and P. De Hert, eds., *Constitutional Rights and New Technologies: A Comparative Study*, (The Hague: Asser Press) 39.

Holznagel, B. and M. Sonntag (2003). 'A Case Study: The JANUS Project' in C. Nicoll et al., eds., *Digital Anonymity and the Law – Tensions and Dimensions* (The Hague: TMC Asser Press) 121-136.

Hostetler, D.R. and S.F. Okada (2013). 'Children's privacy in virtual K-12 education: virtual solutions of the amended Children's Online Privacy Protection Act (COPPA) Rule' 14 North Carolina J L Tech 167-203.

Hui, K. and I. Png (2006). The economics of privacy. In: T. Hendershott (ed.). Handbooks in information systems: Economics and information systems. Amsterdam: Elsevier.

John, L. K., A. Acquisti, and G. Loewenstein (2011). Strangers on the plane: Context-dependent willingness to divulge sensitive information. Journal of Consumer Research 37, 858-873.

Koops, B.-J. (2008). 'Conclusions and Recommendations', in R. Leenes, B.-J. Koops and P. De Hert, eds., *Constitutional Rights and New Technologies: A Comparative Study*, (The Hague: Asser Press) 271.

Koops, B-J. (2014). 'The trouble with European data protection law' 4 International Data Privacy Law 250-261.

Koops, B.-J. & M. Groothuis (2008). 'Constitutional Rights and New Technologies in the Netherlands', in R. Leenes, B.-J. Koops and P. De Hert, eds., *Constitutional Rights and New Technologies: A Comparative Study*, (The Hague: Asser Press) 166.

Kuner, C. (2007). *European Data Protection Law: Corporate Compliance and Regulation* (Oxford: OUP).

Larouche, P. (2013). 'Legal Emulation Between Regulatory Competition and Comparative Law, in P. Larouche and P. Cserne, eds., *National Legal Systems and Globalization – New Role, Continuing Relevance* (The Hague, TMC Asser Press, 2013) 247-287.

Lievens, E. et al. (2008). 'Constitutional Rights and New Technologies in Belgium', in R. Leenes, B.-J. Koops and P. De Hert, eds., *Constitutional Rights and New Technologies: A Comparative Study*, (The Hague: Asser Press) 25.

Lizzeri, A. (1999) Information Revelation and Certification Intermediaries, RAND Journal of Economics, 30: 214-231.

Mayer-Schönberger, V. and K. Cukier (2013). *Big Data* (London: John Murray).

Millard, C. and W.K. Hon (2011). 'Defining "Personal Data" in e-Social Science' 15 Information, Communication and Society 66.

Miller, A. and C. Tucker (2009). Privacy protection and technology adoption: The case of electronic medical records. Management Science 55, 1077-1093.

Miller, A. and C. Tucker (2011). Can healthcare information technology save babies? Journal of Political Economy 119, 289–324.

Miller, A. and C. Tucker (2014). Privacy protection, personalized medicine and genetic testing. Mimeo, MIT.

Narayanan, A. and V. Shmatikov (2009). 'De-anonymizing Social Networks' Publications of 30th IEEE Symposium on Security and Privacy 173-187.

Ohm, P. (2010). 'Broken Promises of Privacy' 57 UCLA L Rev 1701-1777.

Pew Research Center (2014). Public perceptions of privacy and security in the post-Snowden era. Report, November 2014, available at http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/

Posner, R. A. (1981). The economics of privacy. American Economic Review (Papers and Proceedings). 71(2), 405-409.

Prosser, P. (1960). 'Privacy' 48 Cal L Rev 383.

Purtova, N. (2010). 'Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights' 28 Neth Q Human Rights 179-198.

Purtova, N. (2011). *Property in personal data: a European perspective* (Deventer: Kluwer Law International).

Reding, V. (2012). 'The European data protection framework for the twenty-first century' 2 International Data Privacy Law 121.

Regan, P.M. (1995). *Legislating Privacy* (Chapel Hill: University of North Carolina Press).

Rouvroy, A. and Y. Poullet (2009). 'The Right to Information Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in S. Gutwirth, P. De Hert and Y. Poullet, eds., *Reinventing Data Protection* (Springer) 45-76.

Samuelson, P. (2000) 'Privacy as Intellectual Property?' 52 Stanford L Rev 1125-1173.

Schwartz, P. (2009) 'Preemption and Privacy' 118 Yale L.J. 902-947.

Schwartz, P. and J.R. Reidenberg (1996). *Data Privacy Law: A Study of United States Data Protection* (Charlottesville: Michie).

Schwartz, P. and D.J. Solove (2011). 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' 86 NYU L Rev 1814-1894.

Schwartz, P. and D.J. Solove (2014). 'Reconciling Personal Information in the United States and European Union' 102 California L Rev 877-916.

Solove, D.J. (2001). 'Privacy and Power' 53 Stanford L Rev 1393-1462.

Solove, D.J. and W. Hartzog (2014). 'The FTC and the New Common Law of Privacy 114 Columbia L Rev 583-676.

Solove, D.J., M. Rotenberg and P. Schwartz (2006). *Information Privacy Law*, 2nd ed. (Aspen Publishing).

Stigler, G. J. (1980). An introduction to privacy in economics and politics. Journal of Legal Studies 9(4), 623-644.

Taylor, C. (2005). Privacy and information acquisition in competitive markets. Unpublished manuscript, Duke University.

Taylor, M. (2012). *Genetic Data and the Law* (Cambridge: Cambridge University Press).

Tene, O. and J. Polonetsky (2012). 'Privacy in the age of Big Data' 64 Stan L Rev Online 63.

Tiebout, C.M. (1956). 'A Pure Theory of Local Expenditures' 64 J Pol Econ 416-424.

Tucker, C. (2014). Social networks, personalized advertising, and privacy controls. Journal of Marketing Research 51(5), 546-562.

Turow, J. , J. King, C. Hoofnagle, A. Bleakley, and M. Hennessy (2009). Americans reject tailored advertising and three activities that enable It. Unpublished manuscript, available at http://repository.upenn.edu/asc_papers/137.

Warren, S.D. and L.D. Brandeis 'The Right to Privacy' (1890) 4 Harv L Rev 193-220.

Whitman, J.Q. (2004). '.Q. (2004). 3 L Rev 193edu/asrivacy: Dignity versus Liberty' 113 Yale L.J. 1151-1221.

Xu, H., H.-H. Teo, B. C. Y. Tan, and R. Agarwal (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. Information Systems Research.