9 FROM COLLECTION TO USE IN PRIVACY REGULATION? A FORWARD-LOOKING COMPARISON OF EUROPEAN AND US FRAMEWORKS FOR PERSONAL DATA PROCESSING

Joris van Hoboken

9.1 INTRODUCTION

How are we to ensure respect for information privacy in the 21st century? Answering this question, some have put forward the argument that regulation should focus on the use of data instead of its initial collection (Mundie 2014; White House 2014a; White House 2014b; Cate et al. 2014; Landau 2015; World Economic Forum 2013). The main argument for this shift tends to be pragmatic, namely that the collection of personal data has become the normal state of affairs. As a result, focusing the regulation of personal data-driven processes by limiting the collection of data (data minimization) is no longer feasible and desirable. Regulation should focus on issues arising from the actual use of personal data instead.

The arguments for use regulation tend to involve two specific elements. First, the existing mechanisms for establishing the *legitimacy* of personal data collection and further use (in view of information privacy) need to move away from a negotiation at the time of collection, in terms of specified, legitimate purposes, towards a focus on data use and management practices. Second, a use-based approach could provide the *flexibility of re-use of data* across contexts, which is argued to be required to extract the optimal value from data analytics. Cate et al. (2014) argue:

> "The evolution of data collection and data use necessitates an evolving system of information privacy protection. A revised approach should shift responsibility away from individuals and toward data collectors and data users, who should be held accountable for how they manage data rather than whether they obtain individual consent. In addition, a revised approach should focus more on data use than on data collection because the context in which personal information will be used and the value it will hold are often unclear at the time of collection" (Cate et al. 2014).

The resulting debate about regulatory flexibility for Big Data analytics may be one of the core data privacy debates of our time. On one side of the debate are those that propose more flexibility for the further processing of personal data for new unanticipated purposes (at the moment of collection) in view of the opportunities of data analytics. For example, the German Member of the European Parliament Voss recently argued: "there is one necessary condition for enabling innovation to flourish: allowing data to be processed without a pre-determined purpose" (Voss and Padova 2015).

On the other side of this debate about information privacy principles are those that remain committed to the basic principle that data processing purposes and their legitimacy should be established from the moment of collection of personal data. Other authors have questioned the European focus on data minimization in view of its minimal impact in practice but have argued for different regulatory solutions. As Koops (2014) argues:

> "the Data Protection Directive has done little to prevent the development of massive databases or the advent of the Big Data era, and it is folly to think that the GDPR will fare better in preventing 'unnecessary' data processing. Who in his right mind can look at the world out there and claim that a principle of data minimisation exists?".

Koops (2013) argues that, in a world of data analytics, regulation should increasingly focus on decision transparency to be able to guarantee due process and fair treatment of individuals.

This article will look at the position advocating use-based regulation as an alternative for restrictions on collection, from a transatlantic comparative legal and policy perspective. It will first look at the legal question about the position of the related principles of purpose limitation, data minimization and the question regarding the legitimacy of personal data processing in the European and US privacy regimes and make an assessment of the impact of existing regulatory frameworks on industry and government practices. On this basis, it will explore the viability and consequences of a possible shift towards a focus on the use of personal data in the information society. It will put this discussion in the context of current developments in Europe and in the United States. While focusing mostly on the commercial context, the article will also discuss collection and use from a government perspective, including the question of constitutional rights to information privacy and their consequences for collection and use in privacy law and policy.

The following two main questions will be specifically addressed. First, what is the current position of data minimization (and restrictions on the collection of personal data) in existing legal frameworks for data privacy, in Europe and in the US? As a considerable divide can exist between privacy law in the books and privacy law in practice, this question will be answered with reference to the impact of data minimization in practice. Specific reference will be made to legal developments affecting the central position of collection in the regulation of personal data processing, including the debate about the adoption of a new EU General Data Protection Regulation. Second, what are the rationales underlying a focus on collection and to what extent do these rationales remain valid? This also involves the question whether the regulation of the use of personal data can be considered as an alternative for the regulation of the collection of personal data.

For the purposes of this article, collection is broadly defined as whether a particular entity has access to or control over (personal) data for any potential use. Purpose limitation is understood as the principle that personal data must be processed for specified, explicit and legitimate purposes and not further processed in ways that are incompatible with those purposes. Data minimization is understood as the principle that the processing of personal data, including its collection, should be kept at a necessary minimum. Use of personal data is defined as any kind of use of personal data by a particular entity, including the transfer of data to third parties.

9.2 COLLECTION AND USE IN EUROPE

The primary legal data privacy instrument in Europe is the Data Protection Directive (95/46/EC, DPD), which harmonized data privacy legislation in the Member States. The dual aim of the DPD was to protect "the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data", while ensuring that such protection would "neither restrict nor prohibit the free flow of personal data between Member States" (Article 1 DPD). Proposals to replace the DPD with a General Data Protection Regulation (GDPR) have been debated at the EU level since 2012 (European Commission 2012, European Parliament 2014, Council 2015)[1] and were *de facto* adopted in December 2015.[2]

The DPD and its implementations in the Member States exist against the backdrop of fundamental right protection of data privacy at the EU level and within the Council of Europe and the international context. Article 8 of the European Convention on Human Rights (ECHR) includes protection of data privacy. Notably, the scope of the right to private life of Article 8 is wide, but not all personal data processing is covered (FRA 2014). Article 8 ECHR not only applies to interferences by public authorities but also entails positive obligations on public authorities to ensure respect for the protection in horizontal relations, which the DPD can be considered to effectuate. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) adopted in 1981, is the first regional framework for the processing of personal data and applies to all personal data processing in the public and private sector, including for law enforcement and national security.

Since the Lisbon Treaty entered into force in 2009, the EU data privacy regime in the DPD has been further anchored at the fundamental rights level in the EU Charter (Fuster 2014). The EU Charter contains a separate binding right to the protection of personal data (Article 8), alongside the protection of private life, family life

and correspondence (Article 7). Article 8 of the Charter on the 'Protection of personal data' provides protection for personal data processing, including collection, and stipulates that:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

The DPD applies to the processing of personal data in the private sector as well as the public sector, with certain exceptions, including the processing of personal data by law enforcement and national security agencies.[3] Personal data is defined broadly as "any information relating to an identified or identifiable natural person ('data subject')", where "an 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" (Article 2(a) DPD). The DPD imposes a set of interlinked obligations on the processing of personal data by data controllers, i.e. the entity "which alone or jointly with others determines the purposes and means of the processing of personal data" (Article 2 DPD). Basically, any operation one could perform on data, including collection, storage, organization and disclosure or transfer to third parties falls within the definition of processing. The DPD also applies to personal data that have been made public. In view of freedom of expression, Member States are required to adopt exceptions and derogations to the "processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression" (Article 9).

Data minimization, i.e. keeping the processing of personal data at a necessary minimum, is a core principle of the existing European legal data protection framework. It follows from a combination of the principle of purpose limitation and the requirement of a legitimate ground. With respect to purpose limitation, Article 6 DPD provides that personal data can only be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." It also requires that the personal data should be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed", "accurate and, where necessary, kept up to date" and "kept in a form which permits identification of data subjects for no longer than is necessary

for the purposes for which the data were collected or for which they are further processed." Recital 28 provides that the purposes "must be determined at the time of collection of the data."

The DPD does not contain the assessment criteria whether further processing is incompatible with the purposes for which the data were collected. Member States have developed these criteria in specific national legal provisions, including "the relationship between the purposes for which the data have been collected and the purposes of further processing", "the context in which the data have been collected and the reasonable expectations of the data subjects as to their further use", "the nature of the data and the impact of the further processing on the data subjects" and the "the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects" (Article 29 Working Party 2013a: 23-27).

There are exceptions to the principle that data should only be processed for compatible purposes. First, Article 13 DPD stipulates that Member States can provide for exceptions to the further processing of personal data, including for law enforcement and national security. Typically, lawful access regimes in the Member States do provide for such exceptions. Second, an exception applies to the "further processing for historical, statistical or scientific purposes." Such processing may take place as long as 'appropriate safeguards' are implemented. Recital 29 of the DPD specifically provides that these safeguards must "rule out the use of the data in support of measures or decisions regarding any particular individual."

In practice, it appears that the exception for statistical and scientific purposes is used for data mining by commercial entities and the development of group profiles (Article 5.3.2 Dutch Code of Conduct Financial Industry 2010). As these group profiles tend to be used to support subsequent decision making regarding data subjects, this raises questions about the interpretation and enforcement of this recital in current legal practice. The GDPR provides for more flexibility with respect to the further processing of personal data for historical, scientific and statistical purposes. Recital 29 of the DPD, which the EDPS still recommended to include in the text of the GDPR, has been deleted from all official versions of the current text (EDPS 2015). On the question of the status of group profiles, the GDPR provides an ambiguous answer. Article 20(1) of the GDPR could be read in a way that it covers the processing of group profiles, but the rest of Article 20 suggests otherwise, and the scope of the GDPR generally remains restricted to the processing of personal data, thus leaving the larger issue of profiling unaddressed (Koops 2014: 257-8).

The strength of the data minimization principle depends on which data processing purposes, to be stipulated by the data controller at the time of collection, can be considered legitimate. This question is answered in general terms in Article 7 DPD, which lists six possible legitimate grounds for the processing of personal data.

Four of these grounds are framed in terms of whether the processing is 'necessary' for a generally accepted purpose for the processing of personal data. This includes that the processing should be necessary for "the performance of a contract to which the data subject is a party" (sub b), which is a primary ground for data processing in the private sector. For the public sector it provides the legitimate grounds that the processing is "necessary for compliance with a legal obligation to which the controller is subject" (sub c) or "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed" (sub e). In addition, data processing is legitimate if it "is necessary in order to protect the vital interests of the data subject" (sub d).

There are two additional legitimate grounds of a somewhat different nature. Article 7 (f) provides for a balancing test, requiring that the processing:

> "is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject [protected by the DPD]."

The balancing test in Article 7(f) provides particular flexibility in practice for the private sector. It does not require controllers to conduct the balancing in a transparent manner, making it hard to challenge for data subjects (Bits of Freedom 2012).

Article 7(a) provides for the legitimate ground that "the data subject has unambiguously given his consent", which is increasingly portrayed as the primary legitimate ground for the processing of personal data. In early data privacy laws in Europe, the consent of the data subject played a more limited role (Kosta 2013: 383-384; Fuster 2014: 137). The DPD and even more so the proposals for the GDPR, however, placed increased emphasis on consent, connecting to the understanding of data privacy as control over one's personal data (Westin 1970; European Commission 2012). The new fundamental right to the protection of personal data in the EU Charter (Article 8) also gives consent a central role (Fuster 2014: 204).

Still, the function of consent remains limited to the legitimate ground test. The other requirements in the DPD or the GDPR are not dependent on the consent of the data subject, including that personal data are only processed fairly,

transparently, for compatible specific explicit purposes, stipulated from the time of collection, that controllers respect data subject's rights to access, correction and deletion, all of which are subject to oversight by the Data Protection Authorities.

To summarize the above and its consequences for the regulation of the collection of personal data, the DPD regulates the processing of personal data from the moment of collection, but it does not regulate collection in the sense that it strictly prevents the collection of personal data. Except for the processing of sensitive data, the DPD does not prohibit personal data collection and further processing, but places it under many flexible general conditions, many of which are procedural.

Thus, the general DPD regime for the processing of personal data can best be characterized as 'yes, you can collect and process personal data as long as.' In sum, we may have to answer Koops's remarks about data minimization cited in the introduction with the conclusion that the current European model was never designed to prevent the 'development of massive databases or the advent of the Big Data era' (Koops 2014). It merely aimed to put some reasonable conditions on the collection and processing of personal data, including that they are collected for acceptable purposes. This does not mean that there is no data minimization principle. It just means that this principle does not stand in the way of legally permissible large-scale personal data processing activities.

To illustrate this, a data controller can easily maximize the amount of personal data it can legally collect and use by stipulating a large variety of data processing purposes that it is ready to defend as legitimate on the basis of Article 7 DPD. For data-intensive services or organizations, this would amount to a long list of data processing purposes, ranging from specific legal requirements to monitoring of fraud and abuse, monetization and the offering of specific personalized service features. It would indeed be a stretch, therefore, to argue that a *strict* principle of data minimization exists in the current regime. Clearly, the available legitimate grounds can flexibly cover a large range of reasonable processing purposes that private and public sector data controllers tend to be involved in.

The DPD regulates the use of personal data by requiring that the further use that is made of personal data is compatible with the specific, explicit and legitimate purposes for which the data were collected. As mentioned, the further use of personal data for historical, statistical or scientific purposes is not generally considered incompatible and permitted as long as appropriate safeguards have been applied. Another specific example of use regulation in the DPD is the provision on automated decision-making in Article 15. This provision reads as a prohibition of decisions with regard to data subjects that are solely based on processing of personal data that produce legal effects or significantly affect her or him. The DPD further

gives data subjects the right to obtain "knowledge of the logic involved in any automatic processing of data" in such uses of personal data. The GDPR text on protection against profiling in Article 20, discussed above, is based on Article 15 DPD.

The legislative documents relating to the GDPR showed a general willingness to relax the existing restrictions on the further use of personal data once they have been collected. The EC proposal explicitly includes the principle that personal data be "limited to the minimum necessary in relation to the purposes for which they are processed" (Article 5(c), replacing the 'not excessive' language from the DPD in Article 6 (European Commission 2012). Some might conclude from this that the EC aims to strengthen the data minimization principle, but whether this is the case depends on the interpretation of necessity and legitimate purpose. More importantly, the EC proposes that processing for incompatible purposes would be allowed in the future, outside of the existing exceptions, as long as consent would be obtained or the incompatible processing could be based on another legitimate ground for processing (European Commission 2012, Article 6(4)). As noted by the EDPS, this proposal would open up "broad possibilities for re-use of personal data in particular in the public sector" and would blur the distinction between the cumulative requirements of purpose limitation and legitimate ground for processing of personal data (EDPS 2012: 123). It also places the requirement that "purposes should be explicit and legitimate and determined at the time of the collection of the data" in a new light (European Commission 2012, Recital 30). The European Parliament proposes to delete the proposed Article 6(4), staying closer to the current regime (European Parliament 2014).

The Council's General Agreement went a step further than the Commission in relaxing restrictions on incompatible use. It proposed that "further processing for incompatible purposes on grounds of legitimate interests of the controller or a third party shall be lawful if these interests override the interests of the data subject" (Council 2015, Article 6(4)). Moerel and Prins argue in favour of these proposals by the Council and conclude that it is "the only feasible way to guarantee a future-proof mechanism" (Moerel and Prins 2015). The EDPS (EDPS 2015), the Article 29 Working Party (Article 29 Working Party 2015a) and a large coalition of civil society organizations (McNamee 2015) warned against the further erosion of purpose limitation and the use of this balancing test to sanction uses of data incompatible with the purposes for which they were collected.

The Dutch Government anticipated this possible relaxation of purpose limitation in its exploratory proposals for a Framework Act for data-driven collaborations in the public sector. This Framework Act aims to provide the necessary legal basis for collaboration between different entities to exchange personal data, even if the resulting exchange would be incompatible with the purposes for which the respective agencies had collected them (Kaderwet 2015: 12). A specific use that the law

would facilitate is combining data sets to develop risk profiles and apply these to the respective data sets. In addition, it would override confidentiality requirements and other provisions in specific public sector data processing regulations limiting the sharing of personal data with other entities, including private parties. As the exploratory report states:

> "With respect to disclosure for such collaborations, the confidentiality requirements in these sectorial laws focus on 'no, unless'. A framework act could tilt this paradigm to 'yes, unless'" (Rapport Verkenning Kaderwet 2014: 34).

Notably, without the changes to the possibility of further processing for incompatible purposes, as included in the EC proposal and the Council's General Agreement, this proposed regime in the Netherlands would be incompatible with European Law.

The ongoing enforcement actions of national data protection authorities with respect to Facebook and Google can help to illustrate the current regime for the private sector in Europe. When we review the available documents, it becomes clear that for purpose limitation to function as a meaningful check on personal data processing activities, it is essential that controllers be specific enough about their actual data processing purposes. Otherwise, it is impossible for regulators to make an assessment of the legitimate ground as well as the restriction on further processing for incompatible purposes. However, not unlike many other data controllers, Google and Facebook communicate about their purposes for the processing of personal data in vague general terms and appear to formulate those purposes in a way to optimize their legal space for the combination and further use of data, once collected. Consider the conclusion form a recent study from the University of Leuven for the Belgian Privacy Commission with respect to Facebook:

> "Overall, Facebook's revised [Data Use Policy] signals the company's data use practices in a more prominent way. In this regard, Facebook seems to have taken an important step forward. However, the uses of data are still only communicated on a general and abstract level. Much of the [Data Use Policy] consists of hypothetical and vague language rather than clear statements regarding the actual use of data" (Van Alsenoy et al. 2015: 10).

With respect to Google, the Dutch Data Protection Authority explains in its 2013 report that it "has distinguished four actual purposes, and ascertained that these are so vague or broad that during the collection process they cannot provide any framework against which it can be tested whether the data are necessary for that purpose or not." At the end of 2014, the Dutch DPA decided to impose a cease and desist order on Google, partly based on the following conclusion:

> "Google acts in breach of Article 7 of the Dutch Data Protection Act, which proscribes that personal data are collected for specific and legitimate purposes, because the evaluated purpose specifications in the Google Privacy Policy and the newly mentioned purpose by

> Google of 'the provision of the Google Service' are not well defined and insufficiently specific and because Google does not have a legitimate ground for the processing of the personal data for the assessed four purposes" (Dutch Data Protection Authority 2014).

In other words, even after enforcement pressure, Google and Facebook have not yet been willing to disclose specific enough information about their processing purposes for purpose limitation to fulfil its designated role. Notably, these data controllers do not choose the strategy of formulating a long list of purposes, as discussed above, but a more problematic strategy of formulating a small set of vague broad purposes, shielding their specific data use practices from a thorough legitimacy assessment by data subjects and regulators. In other words, the purpose limitation principle may already have to be taken with a grain of salt in practice. This may partly be explained by the lack of enforcement powers and capacity, which the GDPR revisions aimed to address. At the same time, however, the GDPR could provide more flexibility to the changing and reformulation of purposes, as discussed above, making the impact of the GDPR on these practices difficult to assess.

To conclude this section on collection and use in the European data privacy context, it is worth discussing the case of mandatory retention of electronic communication data. This phenomenon exists on the interface of private and public sector personal data collection practices and raises particularly interesting questions with respect to the question of collection and use in data privacy regulation. Specifically, the recent judgment of the Court of Justice of the European Union (CJEU) in *Digital Rights Ireland*, in which it struck down the Data Retention Directive (DRD), provides some guidance on the position of collection and use in an assessment related to the fundamental rights to private life and the protection of personal data (CJEU 2014). More generally, this judgement illustrates the significance of the EU Charter for the protection of data privacy in the European legal order.

Data retention fits in a wider trend in which governments optimize their ability to exercise power and control on the basis of private sector data (Prins et al. 2011: 96-97). In the Netherlands, for instance, a series of laws have been put in place that facilitate access by law enforcement authorities to any type of data held in the private sector.[4] These laws build on the exception to purpose limitation in Article 13 DPD, making it possible that data collected for the purpose of providing a commercial service end up being used in criminal investigations. Dutch criminal procedural law provides for lawful access by law enforcement to almost any kind of personal data held by others if the data are relevant to an ongoing investigation. Only in cases of sensitive data is there a need for a check by a judicial authority (Van Hoboken 2006).

Agencies other than law enforcement, such as the Dutch Tax Administration, have considerable data collection powers as well, as illustrated most recently in the debate over lawful bulk collection of data of an automated parking service, SMS Parking (Court of Appeals Den Bosch 2014). Once collected by the Dutch Tax office, these data also become available to Dutch law enforcement and intelligence agencies (Martijn 2014). Recent proposals for a new Dutch law for the intelligence agencies provide for broadened powers to gather data from private and public sector entities, including bulk and direct access (Ministerie van Binnenlandse Zaken 2015, Artikel 22). Finally and unfortunately, the shadow of government access to private sector data does not limit itself to national borders. Internationally operating companies can be approached by government agencies abroad to access data of individuals residing elsewhere, regardless of legal process and substantive requirements in their proper jurisdictions (see Van Hoboken et al. 2013).

The DRD went one step further than laws facilitating mere government access, by requiring that electronic communications traffic and location data would continue to be stored, even if the data were no longer necessary for private sector purposes, for a period between 6 and 24 months. The basic rationale of data retention is that data should be retained to ensure their availability to public authorities, in case the respective data should be relevant to a future investigation. Thus, data retention legitimizes collection in view of *potential* future use, putting additional stress on the purpose limitation principle.

The CJEU invalidated the DRD in its *Digital Rights Ireland* judgment because of its incompatibility with the Charter.[5] The CJEU established that the directive's retention obligation amounted to a wide-ranging and particularly serious interference with Articles 7 and 8 of the Charter. The CJEU did not consider the essence of the rights affected as the directive did not apply to communications content (Article 7 Charter) and imposed obligations to implement measures "against accidental or unlawful destruction, accidental loss or alteration of the data" (Article 8 Charter).[6] The CJEU subsequently concluded that the "retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest"(par. 44).

The Court's invalidation of the Directive was the result of its application of a strict proportionality test, in which it observed a general lack of limitations, exceptions and possible safeguards in the DRD. The CJEU noted specifically how the directive affected 'all persons using electronic communications services' and applied 'even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime' (par. 58).

In addition, it signalled that it would expect a much more granular legitimation for the retention of the relevant data in terms of its likely possible use, noting that the directive did:

> "not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (I) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (II) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences" (par 59).

These considerations place any general data retention mandate (regarding personal data that is particularly revealing with respect to the private life of individuals) in a suspect light, as such general data retention laws precisely follow the logic that they allow these links to be established after the potentially useful data has been collected. What is at issue, therefore, in the Court's perspective on the fundamental rights to privacy and the protection of personal data, is the mere collection and retention of the data.[7]

9.3 COLLECTION AND USE IN THE UNITED STATES

US privacy law is a fairly complicated area of legal doctrine, consisting of a combination of specific privacy torts, sectoral and state level data privacy laws for the private sector as well as a number of public sector related privacy laws, including the Privacy Act and legal rules relating to government access to data and communications. In contrast to the European omnibus data privacy law model, US data privacy law is characterized by a sectoral approach to legislating modern data privacy issues (including through self-regulation) as well as the adoption of information privacy law at the State level. An initial omnibus bill for the public and private sector was introduced in 1974, but not adopted (Schwartz 2009: 910-913). Instead, Congress adopted the federal Privacy Act for the public sector and a series of sectoral laws for the private sector, including the Fair Credit Reporting Act (FCRA) of 1970, the Family Educational Rights and Privacy Act of 1974, the Right to Financial Privacy Act of 1978 and the Video Privacy Protection Act of 1988. Discussions to adopt some form of omnibus protection of information privacy remain ongoing – most recently a Consumer Privacy Bill of Rights was proposed by the White House – but have been unsuccessful until now.

In comparison with Europe, whose approach is often characterized in the US as an approach seeing privacy as a fundamental right, relevance of constitutional privacy safeguards in the US is relatively limited. The US Constitution does not recognize a general fundamental right to private life or a right to protection of one's personal data, but several provisions in the US Bill of Rights protect certain elements of a

more fundamental right to privacy. US legal doctrine generally does not recognize the existence of positive state obligations to protect or establish horizontal effect of constitutionally protected rights of individuals.

The First Amendment can entail protection of certain personal data against government collection, if such collection would interfere with the First Amendment's protection of freedom of speech and freedom of association (Strandburg 2008; Solove 2010). The Fourth Amendment protects against unreasonable searches and seizures, requiring the issue of a warrant on probable cause. Arguably, this is a stricter requirement than the flexible proportionality test required by Article 8 ECHR or the EU Charter.

A reason for increased attention to the implications of the First Amendment for government surveillance is that the Fourth Amendment provides only a weak check on government data collection practices. The protection of the Fourth Amendment against government surveillance is limited in several respects by the case law of the US Supreme Court, most notably by the so-called third-party doctrine. Under an aggressive interpretation of this doctrine, individuals generally do not enjoy the protection of the Fourth Amendment for information held by or turned over to third parties. In a world of Big Data and comprehensive sets of personal data relating to all aspects of social and economic life, the doctrine severely restricts the Fourth Amendment's impact on the US government's personal data collection practices. Although this strict interpretation of the third-party doctrine is still widely defended in US scholarship (see e.g., Kerr 2009), a growing body of legal scholarship and judicial opinions, Justice Sotomayor's concurrence in *US v. Jones* in particular, points towards a more nuanced answer to the question of reasonable expectations of privacy in records held by third parties (Strandburg 2011; Baer 2014).

If we take a look at the third-party doctrine from the perspective of the collection versus use debate, a number of observations can be made. First, the third-party doctrine entails an interpretation of the Fourth Amendment's focusing almost exclusively on the (initial) collection of data as the relevant issue. Once data has been disclosed to third parties, Fourth Amendment protection is no longer applicable, on the rationale that it implies consent (Kerr 2009: 565). In the face of such reasoning, the idea that collection of data should no longer be the law's focus in protecting the right to privacy is unpersuasive. If anything, a continued adherence to the third-party doctrine means that collection of one's data by a third party is precisely something to worry about because collection implies the loss of constitutional protection. The alternative to such protection is for the US legislature to adopt statutory protections that afford privacy protections against unrestrained government collection. Such statutory protections do exist for some specific

categories of information held by third parties. Examples are the Right to Financial Privacy Act adopted in response to *Miller* and the Pen Register and Trap and Trace Devices Statute adopted in response to *Smith*.

In the consumer privacy context, the Federal Trade Commission has used its authority with respect to unfair and deceptive business practices to develop an increasingly robust information privacy doctrine at the federal level (Solove and Hartzog 2014). The FTC has been the dominant federal agency involved in addressing privacy issues in the online context through self-regulatory initiatives and has authority to oversee and enforce an increasing number of privacy regulations. Indeed, the FTC has become the *de facto* Data Protection Authority in the US for the consumer privacy context (Solove and Hartzog 2014): first, it has applied the unfair and deceptive business practices to personal data collection and use. Second, it has recommended various versions of the Fair Information Practices to shape self-regulatory initiatives to address privacy issues in different sectors of commerce, including online advertising and data brokerage. Finally, it has enforced statutory laws, including the FCRA, the Safe Harbor Agreement with the EU, and the Children's Online Privacy Protection Act (COPPA).

In its self-regulation initiatives, the FTC has been influenced by the framework of Fair Information Practice Principles, notice and choice in particular, but it has not strongly endorsed a collection limitation or purpose specification and limitation principle.[8] A set of five Fair Information Practice Principles (FIPPs) were first proposed in the 1970s by the Department of Health Education and Welfare and included the principle that: "there must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent" (US Department of Health 1973). An international version of the FIPPs was developed in the OECD context and consisted of eight principles, including the 'collection limitation principle' and the 'purpose specification principle'. These principles do not appear in recent FTC recommendations, such as the slimmed-down set of four FIPPs for online privacy (Strandburg 2014: 6-8), with only the two core principles (notice and choice) having implications for data collection and use:

1. Notice: Websites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.

2. Choice: Websites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).

FTC privacy doctrine does provide some regulatory tools to prevent data from being used for new unexpected purposes. In this regard, the establishment of the notice principle (in self-regulation in combination with statutory and Safe Harbor requirements on privacy policies and notification) has had positive synergies with the FTC's deception standard. Once the practice of privacy policies was established, the deception standard allowed the FTC to take action against misrepresentations about the use of data. Furthermore, the FTC's doctrine of deception has moved beyond policing broken promises. It now also includes "a general theory of deception in obtaining personal information and deception due to insufficient notice of privacy-invasive activities" (Solove and Hartzog 2014: 627-638).

Notwithstanding the progress the FTC has made in establishing a more robust data privacy regime in the US, filling the large legal gaps left by sectoral statutory law, the notice and choice regime of privacy self-management has been widely criticized for being ineffective, for overburdening individuals and for being a procedural sidestep on substantive questions about the legitimacy of personal data processing (see e.g., Solove 2013; Barocas and Nissenbaum 2014). In practice, the choice principle is a weak form of consent with respect to personal data processing and is generally satisfied by giving some opt-outs or a simple 'take it or leave it' option. As Grimmelmann has summarized recently, pointing to more general issues with respect to terms of service and contract law:

> "Any attempt to empower consumers – think 'notice and choice' in privacy law – ends up tossing a few more shovelfuls of disclosure onto the contractual dung heap. Now consumers have 'notice' of the practice regulators want them to know about. But their 'choice' is emptier than ever" (Grimmelmann 2015).

There remains a large area of data collection and use untouched by the doctrines and laws mentioned above, including data collected and used in the absence of interactions with data subjects in commercial relations. This largely unregulated area of personal data processing can be illustrated with a short discussion of the phenomenon of data brokers and the attempts of the FTC to impose some checks and balances on this multibillion dollar industry involved in the collection, profiling and sale of personal data (FTC 2014). Data brokers, such as the Acxiom company, collect personal data from a variety of sources, including government records, publicly available sources, including (new) media, and commercial sources of data (including other data brokers). Acxiom reportedly has 3,000 data segments for nearly every US consumer (FTC 2014: 6). Data brokers sell their data for use in

(personalized) marketing as well as for profiling and risk assessment in the private and public sector. Outside specific areas of activity regulated by the FCRA, the collection and use of this information mostly remains a matter of contractual agreements between data sources, data brokers and further users, with minimal levels of transparency and accountability towards data subjects and society more generally.

As the FTC mentions in its study, there are but few laws that regulate the use of certain public records by data brokers, such as state laws that restrict the use of voter registration records for commercial or non-election-related purposes (FTC 2014: 12). Additionally, use restrictions are sometimes made part of contractual agreements by government sources of data:

> "[C]ertain federal or state laws or agencies require a written agreement affirming that the data broker will only use the data for a specified purpose. Sources may also prohibit data brokers from reusing or reselling the data without permission; decoding or reverse engineering the data; illegally or illicitly using the data; and using the data in violation of the FCRA, Gramm-Leach-Bliley Act (GLBA), HIPAA, or Children's Online Privacy Protection Act (COPPA)" (FTC 2014).

The Fair Credit Reporting Act has been mentioned as an example of use-based regulations of personal data; it regulates certain uses of consumer credit information by Credit Reporting Agencies (CRAs). Specifically, the FCRA establishes data protection standards for the issuing of consumer credit reports, i.e. personal data that is collected and combined to evaluate credit, insurance or employment eligibility. It imposes transparency obligations and data subject rights of access and correction and requires that CRAs "follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates" (15 U.S.C. § 1681e, (b)). The FCRA also contains obligations to suppress certain information from consumer reports and requires that CRAs take measures to ensure that information from credit reports is not used for purposes other than the purposes for which it was requested. When CRAs comply with the FCRA's safeguards, they are shielded from liability.

When taken as an example of use-based regulation, the FCRA cannot be considered a resounding success. Hoofnagle concludes that

> "[c]onsumer reporting shows us that while use-based regulations of Big Data provided more transparency and due process, they did not create adequate accountability. Indeed, despite the interventions of the FCRA, consumer reporting agencies (CRAs) remain notoriously unresponsive and unaccountable bureaucracies" (Hoofnagle 2013).

The FCRA singles out a set of data usage in the data broker industry for stricter regulation. Unsurprisingly, the particular scope of the FCRA is contested and the subject of active litigation. Recently, the US Supreme Court has granted certiorari in a case in which a people search engine *Spokeo* was confronted with a class action law suit alleging violation of the FCRA.[9] The case, which currently revolves around the

initial question of standing in information privacy laws like the FCRA, also illustrates the issues that arise from singling out the use of certain information by certain actors for stricter regulation. Spokeo disputes that it can be considered a CRA and warns visitors to its website that "none of the information offered by Spokeo is to be considered for purposes of determining any entity or person's eligibility for credit, insurance, employment, or for any other purposes covered under FCRA" (Spokeo 2014).

Finally, a use-based regulatory approach through statutory laws may run into First Amendment troubles. Several lawsuits have argued, unsuccessfully until now, that the FCRA imposes restrictions on the use of data in violation of the First Amendment or that use restrictions on data could be ignored on the basis of the First Amendment (Hoofnagle 2014). These interpretations of the First Amendment typically follow a line of argument presented by Bambauer as 'data is speech'. Not only 'traditional forms of communication (utterances, journals, movies, and the like)' should be protected, but also the gathering and processing of data more generally because of the First Amendment aims to protect against interferences with the creation of knowledge (Bambauer 2013).

In sum, US law provides for less strict collection limitation in comparison to the European framework in the commercial sphere. It has a number of sectoral laws that regulate certain uses of personal data, such as the FCRA, but these approaches have their limitations. Notably, US law does not legally require a legitimate basis for the processing of personal data. FTC privacy doctrine in combination with privacy policy requirements provides some check on the use of personal data for new purposes through the notice and choice framework. This check, which advocates of use-based regulations of personal data consider outdated in a world of Big Data, is already inapplicable to a mature multibillion dollar industry, which provides a good chunk of the data collection and analytics machinery to a world relying on Big Data. Within this industry, use regulation does play a role, but primarily through contractual agreements between data sources and users, including provisions that existing statutory use limitations will be respected downstream.

9.4 FROM COLLECTION TO USE?

The classic informational self-determination rationale for information privacy regulation is that the collection of personal data enables the exercise of power and can have chilling effects on individual freedom and behaviour, effects which should not only be assessed in terms of the impact on specific individuals but also in view of the values of pluralism and democratic self-governance.[10] This rationale, which is specifically tied to the collection of personal data, is widely accepted in European data privacy jurisprudence and affirmed in fundamental rights case law, including the famous census decision of the German Constitutional Court (BVerfG 65, 1

1983) and the Court of Justice of the EU (Digital Rights Ireland par. 28). Individuals may be worried about the collection of data about them and about the purposes for which these data would be used. Personal data, once collected, could be used in ways that are unfair or make their lives more difficult.

While recognizing that there are legitimate reasons for organizations to collect and use data, data privacy law aims to provide the legal conditions for a negotiation to take place on the question whether the collection of certain data for certain purposes is indeed legitimate and restricts the use of data for other, incompatible purposes. In the European context, this question of legitimacy involves either the existence of informed consent or a proportionality test in view of the fundamental right to privacy and the protection of personal data. In the US context, legitimacy is generally not dependent on a legal test as stipulated in the DPD, and in the consumer privacy context the emphasis has been placed on notice and a weak form of consent, i.e. choice.

As a political project, data privacy law and policy has been centrally concerned with shoring up public trust in the way organizations process personal data (as well as trust in information technologies and services), focusing in particular on the foreseeability of data-processing outcomes (Bygrave 2002: 107-112). This foreseeability, which is also a requirement for interferences with fundamental rights in the European context, is specifically promoted through the principles of purpose specification and limitation. The argument for use regulation generally implies that this negotiation on legitimacy would no longer take place at the moment of collection in terms of purposes in a way that restricts the further use of the data collected. When the question of legitimacy shifts to the question whether some defendable use could be made of personal data in the future, however, much personal data collection easily becomes legitimate in a world of Big Data. It is hard to see how such a framework will provide for the foreseeability of data processing in a similar manner. It would put oil on the slippery slope of data collection and unpredictable further use instead.

As discussed with reference to data retention in Europe and the third-party doctrine in the US, a specific rationale for considering the mere collection of data by organizations as a fundamental privacy issue is that collection in the private sector implies the possible collection and use by government agencies for purposes of law enforcement and national security. Data privacy rules typically provide for exceptions to the principle of purpose limitation for such government collection purposes. It does not matter for which purposes the data was collected in the private sector context. When a law enforcement agency fulfils the statutory requirements for collecting the relevant data, government access can generally take place. This places data collection by other organizations in a particular light that cannot be undone by use-based regulations. In fact, the Snowden revelations have made

people and organizations more acutely aware of this reality than ever. In fact, certain industry players are adopting encryption schemes that prevent certain forms of government access from taking place. This shows that increasing trust by limiting data collection through technical means is a viable strategy for the private sector, in the absence of better safeguards against government collection (Van Hoboken and Rubinstein 2014).

In a way, it almost appears as if the advocates of use-based regulation (as an alternative to the regulation of collection of personal data) believe that the concerns of individuals with respect to mere collection will miraculously disappear and that European constitutional judges will eventually overturn their reasoning about data collection and fundamental rights. Considering the increased importance of personal data processing in all facets of society and the increased benefits as well as risks for data subjects, this seems both an unreasonable expectation as well as an undesirable way forward. Instead, it seems more reasonable to expect that more guarantees will be needed instead of less, to ensure the respect for information privacy and the continued trust in information technologies in a world in which any piece of data that is collected can end up being used for any purpose. In sum, to the extent that the advocacy of use regulation can be characterized as a deregulatory agenda (Hoofnagle 2014), such advocacy is unconvincing.

The criticism of the notice and choice requirement by use-based regulation advocates can be considered in this light as well. The argument that notice and choice puts unrealistic and undue burdens on individuals is actually quite convincing. But what conclusions should be drawn from this criticism? First and foremost, the conclusion would be that notice and choice is, for the most part, not a convincing mechanism for determining the *legitimacy* of data processing activities and that alternatives for establishing this legitimacy are needed. Nissenbaum's theory of privacy as contextual integrity is centrally concerned with establishing such an alternative, in which consent plays a much more limited normative role. Instead, objective information privacy norms should be derived from context-depended values, norms and expectations with respect to personal information flows (Nissenbaum 2009). In this theory, privacy:

> "is a right to live in a world in which our expectations about the flow of personal information are, for the most part, met; expectations that are shaped not only by force of habit and convention but a general confidence in the mutual support these flows accord to key organizing principles of social life, including moral and political ones" (Nissenbaum 2009: 231).

European data protection law, although increasingly preoccupied with informed consent as the primary legitimate ground, entails a theory of legitimate grounds that allows substantive, objective assessments of legitimacy to take place.

The debate about collection and use also illustrates a fundamental tension at the basis of privacy and data protection laws, i.e. the tension between privacy as a right to be let alone, on the one hand, and privacy as the fair data-driven treatment of individuals, on the other. The tension can be illustrated with a simple small data example. Article 41 of the Dutch Data Protection Act gives individuals the right to object to the processing of their personal data for marketing purposes. A paradoxical situation emerges for people requesting the deletion of their data from a specific organization. Instead of their request leading to deletion from the marketer's databases, their data now ends up being lawfully included in the marketer's objectors file (Court of Appeals Amsterdam 2011). This file will help ensure the person will no longer receive marketing messages. But from the perspective of privacy as a right to be let alone, this solution is unsatisfactory as it would require the marketer to stop processing the person's data altogether.

A more general version of this tension emerges when one recognizes that the fair data-driven treatment of individuals may have to involve the processing of additional data to ensure that no undue or unfair treatment takes place. In their discussion of Big Data and discrimination, Barocas and Selbst explain that protection against undue discrimination in data mining may sometimes necessitate the collection of more data (Barocas and Selbst, forthcoming). Van der Sloot has argued for data *minimum*mization (instead of minimization), proposing that a minimum of data is collected, stored and clustered, in particular metadata establishing the context of the data, to ensure fair personal data processing through knowledge discovery (Van der Sloot 2011). Interestingly, these arguments seem to imply that purpose specification and limitation would be more important than ever because the legitimacy of such additional data collection in view of fair treatment of data subjects can be much more easily established if the data is only and specifically used for the promised beneficial purposes.

Within boundaries, it is appropriate that data privacy laws allow for the collection and use of additional data to ensure fair data-driven treatment. At some point, however, the argument for more and richer data for a better world will cease to be convincing. For instance, it would be hard to accept the bulk collection of large troves of personal data simply to ensure that no innocent people are convicted of crimes. While some Big Data enthusiasts may embrace the value of bad and messy data (Hoofnagle 2013: 5), this can hardly mean that data privacy law should simply allow the processing of incorrect data, undoing the principle of information quality in data privacy altogether.

The collection and use debate may be best summarized as being about establishing new frameworks for determining the legitimacy of large data processing infrastructures. Considering the historical role of data protection law, it is also about establishing new frameworks for achieving general societal acceptance for personal

data processing taking place in the private and public sector. The use-based regulation approach would not only radically shift the balance between competing legal principles underlying the right to privacy as a right to be let alone towards the fair and legitimate processing of personal data. In the process, it would also erode the legitimacy assessment currently in place for the processing of personal data, applicable from the moment of collection. What would take centre stage are requirements for data security, transparency and enforcement of any measures the data controller has taken to ensure the data is only used in the ways it has considered legitimate. What would be left out are legitimate political, social and moral concerns about the ways in which the collection of personal data shapes and affects people's lives from the moment of collection.

The discussion of European data protection law and the GDPR proposals show that some shift in this direction is not unlikely. Specifically, the GDPR, as adopted, is likely to end up providing more flexibility for the re-use of data for purposes incompatible with the purposes established at the time of collection. This remains controversial and problematic in view of the continued Commission's assertions that the GDPR would not undermine the level of protection established by the DPD (MacNamee 2015). A complete reorientation of European data protection to regulating use seems unlikely, however, for a number of reasons. First, as discussed at the beginning of this section, concerns about the collection of personal data remain at the heart of the fundamental right to privacy in European constitutions and the EU Charter. A strong reorientation would make data protection rules incompatible with the fundamental rights framework, creating constitutional turbulence for decades to come. Second, the omnibus character of European data protection law and its hostility towards exceptions has a strong political and institutional link with the project of European integration (Schwartz 2009). It is unlikely, therefore, that essential areas of data processing activities (collection) will be deregulated at the European level.

A use-based regulatory approach to data privacy is more easily compatible with US privacy law. US law already contains various examples of use-based regulation and lacks a general principle of collection limitation, but there are some hurdles. First, use-based regulation would no longer apply the principle of notice and choice at the moment of collection as the primary assessment for establishing legitimacy of data processing in the consumer privacy context. Considering the deep-rooted ideological attachment to the idea of privacy self-management, this transformation could prove to be a difficult and long process. Second, US constitutional law continues to entail the principle, although increasingly controversial, that data collected by third parties generally loses its fourth amendment protection in view of government collection. From a European perspective, the absence of a comprehensive regulatory framework for the activities of data brokers can easily serve as an example of what not to like in use-based regulation. Under US

law, data brokers can collect, combine, analyse and sell their data largely without any transparency and accountability. Use regulation exists, but mostly as a form of contractual agreements between the sources of data and their subsequent users.

It appears fair to assert that underlying use-based regulation advocacy is the belief that the commercial and societal value present in large data collections is too great to continue restricting the lifecycle of personal data. What the proliferation of data analytics in almost every aspect of society means, however, is that there is more rather than less at stake for people than in the 1970s, when these principles were adopted in the face of mounting public pressure and privacy concerns. And much is at stake from the moment of collection, including the abuse of data, data ending in the wrong hands, old and new unpredictable forms of unfair treatment and discrimination and a general exacerbation of power imbalances. In other words, the real challenge is not to weaken existing protections but to find new ones that give new interpretations to the right to privacy in the digital age.

An ongoing orientation of data privacy law as being concerned with establishing restrictions on the collection of data, including the principle of purpose limitation functioning from the moment of collection, does not imply that use-based regulation does not deserve the attention of scholars and regulators. It simply means this should not be seen as an alternative, but rather as a complementary regulatory strategy to ensure fairness and justice in Big Data analytics. Both sides of the debate about collection or use regulation should be able to agree that the challenges of data analytics for the effective protection of data privacy are substantial. Amongst the most challenging may be the fact that the personal data of others may be as significant as one's own data due to predictive analysis and uses (Barocas and Nissenbaum 2014). A convincing answer to this challenge, however, still needs to be developed.

9.5 CONCLUSION

This article has looked at the collection versus use debate from a comparative perspective. Specifically, it has looked at the question of the current and future position of the principle in data privacy law that personal data should only be collected and further processed for specified and legitimate purposes, established at the time of collection of the data. And it has looked at the question whether use-based regulation can be seen as an alternative for regulation focused on limiting data processing from the moment of collection of personal data, considering the rationales for such regulatory approaches.

Ultimately, the collection versus use debate centres on the question of how to establish legitimacy for the processing of personal data. As the frameworks for establishing such legitimacy in Europe and the US are different in various regards,

the use versus collection debate plays out differently in these legal contexts. In general, the European framework is characterized by regulation of all personal data processing from the moment of collection of personal data. The US framework is primarily focused on addressing specific (perhaps the most egregious) data privacy issues, while leaving much to other than legal mechanisms. These differences notwithstanding, the article concludes that there are significant hurdles to refocusing data privacy law towards use-based regulation on both sides of the Atlantic. In Europe, the existing fundamental rights framework is one of these hurdles as well as the omnibus approach to data privacy regulation. In the US, the ideological attachment to notice and choice, a weak form of consent, as well as the third-party doctrine, stand in the way of the radical reorientation proposed by use-based regulation advocates. In addition, the existing experiences with use-based regulation in the US context can hardly be described as a resounding success.

At the core of the debate about collection and use-based approaches to data privacy is an inherent tension between different legal interpretations of the right to privacy, with the right to privacy as a right to be let alone, on the one hand, and the right to the fair processing of personal data, on the other. Data privacy law will have to come to grips with this inherent tension and find ways to respect both rights without undoing either one of them. The most productive way to address this tension would be to see use-based regulation not as an alternative to regulation of collection, but as a complimentary regulatory strategy that can help address some of the new challenges to privacy inherent in the possibilities of large-scale data analytics.

REFERENCES

Alsenoy, B. van et al. (2015) 'From Social Media Service to Advertising Network, a Critical Analysis of Facebook's Revised Policies and Terms', Draft study, commissioned by the Belgian Privacy Commission 31 March 2015, available at: www.law.kuleuven.be/icri/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf.

Article 29 Working Party (2013a) 'Opinion on Purpose Limitation', Brussels.

Article 29 Working Party (2013b) 'Statement on Big Data', Brussels.

Article 29 Working Party (2015a) 'Press Release on Chapter II of the Draft Regulation for the March JHA Council', Brussels.

Article 29 Working Party (2015b) 'Opinion on the Draft Regulation in View of the Trilogue, Press Release', Brussels.

Baer, M.H. (2014) 'Secrecy, Intimacy, and Workable Rules: Justice Sotomayor Stakes Out the Middle Ground in United States v. Jones', *The Yale Law Journal* 123: 393.

Bambauer, J. (2013) 'Is Data Speech', *Stanford Law Review* 66, 1: 57.

Barocas, S. and H. Nissenbaum (2014) 'Big Data's End Run around Procedural Privacy Protections', *Communications of the ACM* 57, 11: 31-33.

Barocas, S. and A.D. Selbst, 'Big Data's Disparate Impact', *California Law Review* 104, (forthcoming).

Bennett, C.J. (1992) *Data Protection and Public Policy in Europe and the United States*, Ithaca and London: Cornell University Press.

Bits of Freedom (2012) 'A Loophole in Data Processing', available at: www.bof.nl/live/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf [11 December 2012].

Bundesverfassungsgericht (1983) BVerfG 65, 1 (*Volkszählung*).

Bygrave, L. (2002) *Data Protection Law: Approaching its Rationale, Logic and Limits*, Information Law Series 10, The Hague: Kluwer Law.

Cate, F.H. et al. (2014) 'Data Protection Principles for the 21st Century, Revising the 1980 OECD Guidelines', available at: https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf.

Cate, F.H. and V. Mayer-Schönberger (2013) 'Notice and Consent in a World of Big Data', *International Data Privacy Law* 3, 2.

CJEU 8 April 2014, Joined Cases C-293/12 and C-594/12 (*Digital Rights Ireland*).

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) adopted in 1981, Council of Europe, Strasbourg.

Council Directive 95/46/EC 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.

Council of the European Union (2015) Council General Approach to the General Data Protection Regulation, as Included in Interinstitutional File 10391/15, 2012/011 (COD), Brussels, 8 July 2015, available at: www.statewatch.org/news/2015/jul/eu-council-dp-reg-trilogue-10391-15.pdf.

Court of Appeals Amsterdam 15 February 2011, ECLI:NL: GHAMS: 2011: BQ4006.

Court of Appeals Den Bosch 19 August 2014, ECLI: NL: GHSHE: 2014: 2803.

Dutch Code of Conduct Financial Industry (2010) 'Gedragscode Verwerking Persoonsgegevens Financiële Instellingen', approved by the Dutch Data Protection Authority on 13 April 2010, *Staatscourant* 6429, 26 April.

Dutch Data Protection Authority (2013) 'Investigation into the Combining of Personal Data by Google', *Report of Definitive Findings*, November: z2013-00194.

Dutch Data Protection Authority (2014) 'Cease and Desist Decision with Respect to Google', The Hague, available at: https://cbpweb.nl/sites/default/files/atoms/files/last_onder_dwangsom_google_privacyvoorwaarden.pdf [17 November 2014].

Dutch Ministry of Security and Justice (2014a) *Brief aan de Tweede Kamer over Verkenning kaderwet gegevensuitwisseling*, 19 December, The Hague.

Dutch Ministry of Security and Justice (2014b) *Rapport Werkgroep Verkenning Kaderwet Gegevensuitwisseling*, 19 December, The Hague.

European Commission (2012) *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 11 final.

European Data Protection Supervisor (2012) *Opinion of the European Data Protection Supervisor on the Data Protection Reform Package*, Brussels, 7 March.

European Data Protection Supervisor (2015) 'Europe's Big Opportunity, EDPS Recommendations on the EU's Options for Data Protection Reform', *Opinion* 3/2015, 27 July.

European Parliament (2014*) Legislative Resolution on the General Data Protection Regulation*, COM(2012) 0011 – C7-0025/2012, Strasbourg, 12 March 2014.

Fair Credit Reporting Act, consolidated text available at: www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf.

Federal Trade Commission (2014) *Data Brokers, a Call for Transparency and Accountability*, May.

Fundamental Rights Agency (2014) 'Handbook on European Data Protection Law', available at: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law_en.pdf.

Gellman, B. (2015) 'Fair Information Practices, Version 2.13', available at: http://bobgellman.com/rg-docs/rg-FIPShistory.pdf [11 February 2015].

Grimmelmann, J. (2015) 'An Offer You Can't Understand', *JOTWELL*, 15 May.

Hoboken, J.V.J. van (2006) 'Wrikken en wegen over gegevens, Een analyse van de weging van het belang van de burger bij de nieuwe regeling voor de strafrechtelijke gegevensvergaring', Master's Thesis in Law under Supervision of L.F. Asscher, Amsterdam: Universiteit van Amsterdam, April 2006.

Hoboken, J.V.J. van, A. Arnbak and N.A.N.M. van Eijk (2013) 'Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad', *Privacy Law Scholars Conference 2013*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2276103.

Hoboken, J.V.J. van and I. Rubinstein (2014) 'Privacy and Security in the Cloud: Some Realism about Technical Solutions to Transnational Surveillance in the Post-Snowden Era', *66 Maine Law Review* 488.

Hoofnagle, C. (2013) 'How the Fair Credit Reporting Act Regulates Big Data', *Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet*, available at: (SSRN) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2432955.

Hoofnagle, C. (2014) 'The Potemkinism of Privacy Pragmatism', *Slate*, 2 September.

Kerr, O. (2009) 'The Case for the Third-Party Doctrine', *107 Michigan Law Review* 561.

Koops, B.J. (2013) 'On Decision Transparency, or How to Enhance Data Protection after the Computational Turn', pp. 196-220 in M. Hildebrandt and K. de Vries (eds.) *Privacy, Due Process and the Computational Turn*, Abingdon: Routledge.

Koops, B.J. (2014) 'The Trouble with European Data Protection Law', *International Data Privacy Law*, Doi: 10.1093/idpl/ipu023.

Kosta, E. (2013) *Consent in European Data Protection Law*, Leiden: Nijhoff Studies in EU Law.

Landau, S. (2015) 'Control the Use of Data to Protect Privacy', *Science* 347, 6221: 504506.

MacNamee, J. (2015) 'EU Commission – Finally – Confirms That Its Promise on Data Protection Will Be Respected', *European Digital Rights*, 22 July.

Martijn, M. (2014) 'Politie en inlichtingendiensten kunnen via een achterdeur bij gegevens van de Belastingdienst', *De Correspondent*, 30 September.

McDowell, D.F., D. Reed Freeman and J.M. Harper (2013) 'Privacy Class Actions: Current Trends and New Frontiers in 2013', *Bloomberg Law* 3, July.

Ministerie van Binnenlandse Zaken (2015) *Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten* 20xx; Consultatieversie.

Moerel, E.M.L. and J.E.J. Prins (2015) *Further Processing of Data Based on the Legitimate Interest Ground: The End of Purpose Limitation?*, Tilburg: Tilburg University.

Mundie, C. (2014) 'Privacy Pragmatism', *Foreign Affairs*, March/April 2014.

Nissenbaum, H. (2009) *Privacy in Context, Technology, Policy and the Integrity of Social Life*, Stanford, CA: Stanford University Press.

Prins, C., D. Broeders, H. Griffioen, A.G. Keizer and E. Keymolen (2011) *iGovernment*, report 86, Amsterdam: Amsterdam University Press.

Roessler, B. and D. Mokrosinska (2015*) Social Dimensions of Privacy, Interdisciplinary Perspectives*, Cambridge: Cambridge University Press.

Schwartz, P.M. (2009) 'Pre-Emption and Privacy', *Yale Law Review* 118, 5: 902.

Sloot, B. van der (2013) 'From Data Minimization to Data Minimummization', pp. 273-287 in B. Custers et al. (eds.) *Discrimination and Privacy in the Information Society*, SAPERE 3, Berlin Heidelberg: Springer-Verlag.

Solove, D.J. (2013) 'Privacy Self-Management and the Consent Dilemma', 126 *Harvard Law Review*, 1880.

Solove, D.J. and W. Hartzog (2014) 'The FTC and the New Common Law of Privacy', *114 College Law Review* 583.

Spokeo (2014) *Petition for a Writ of Certiorari Filed*, available at: http://sblog.s3.amazonaws.com/wp-content/uploads/2014/06/13-1339-Spokeo-Inc.-v.-Robins-Br.-for-Amici-eBay-Inc.-et-al.-Jun....pdf [May 2014].

Strandburg, K.J. (2008) 'Freedom of Association in a Networked World. First Amendment Regulation of Relational Surveillance', *49 B.C.L. Review* 741.

Strandburg, K.J. (2011) 'Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change' 70', *Maryland Law Review* 101.

Strandburg, K.J. (2014) 'Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context' in J. Lane et al. (eds.) *Privacy, Big Data and the Public Good, Frameworks for Engagement*, Cambridge: Cambridge University Press.

U.S. Department of Health, Education and Welfare (1973) *Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens*, Washington DC.

Westin, A. (1970) *Privacy and Freedom*, New York: Atheneum.

White House (2014a) *Big Data: Seizing Opportunities Preserving Values*, Executive Office of the President of the United States.

White House (2014b) *Big Data and Privacy: A Technological Perspective*, Executive Office of the President of the United States, PCAST.

World Economic Forum (2013) 'Unlocking the Value of Personal Data: From Collection to Usage, World Economic Forum, Industry Agenda', prepared in collaboration with *The Boston Consulting Group Industry*.

NOTES

1 The GDPR proposals were made by the European Commission in January 2012 (European Commission 2012). The European Parliament adopted its position in first reading in March 2014 (European Parliament 2014). The Council finalized its General Approach in Spring 2015 (Council of the European Union 2015). On this basis, the institutions have started their trialogue negotiation process, which they aim to conclude before the end of 2015, in which case the GDPR could be officially adopted in early 2016. The EU data protection supervisor EDPS has issued its own set of detailed recommendations with respect to the proposed GDPR in July 2015 (EDPS 2015).

2 Regulation No XXX/2016, 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). Consolidated text available at www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-1739884. The GDPR will enter into force two years after its official adoption, in early 2018.

3 With respect to the processing of personal data by state bodies for national security and intelligence, the EU generally does not have any competence. There are a number of EU level instruments with respect to the protection of personal data in the law enforcement context and with respect to specific EU level data processing systems related to immigration and policing. Together with the proposals for a new Regulation replacing the DPD, an EC proposal was made for a new Directive for the protection of personal data in the law enforcement context, providing for more harmonization at the EU level. A discussion of these instruments goes beyond the scope of this article.

4 For a discussion of these laws and the policy and scientific debate leading up to them, see Van Hoboken 2006.

5 National data retention obligations remain in place in a number of European member states, including the UK.

6 This consideration about the core of the right to data protection is somewhat surprising. The fact that these particular measures to prevent loss or destruction of data seem to have been included in the Directive in view of the value of the data for government agencies and not in view of data privacy of individuals concerned seems to have escaped the CJEU's attention.

7 Or, in the words of the Advocate General, what requires "the utmost vigilance [is] the actual collection and retention of the data at issue, as well as the data's impact on the right to privacy […]". AG Opinion 12 December 2013, CJEU, C-293/12 (*Digital Rights*), par. 59.

8 For a review of endorsement of different versions and sets of Fair Information Practice Principles by the FTC, see Gellman 2015.

9 For a discussion of the increasing occurrence of privacy class action litigation in the , see McDowell et al. 2013.

10 On the question of the social and collective value of privacy, see recently Roessler and Mokrosinska (eds.) 2015. Nissenbaum's theory of privacy as contextual integrity also emphasizes the (context-dependent) social, political and moral values inherent in the right to privacy (Nissenbaum 2009).