INTERNET POLICY REVIEW
Journal on internet regulation

Volume 5 | Issue 1

Beyond consent: improving data protection through consumer protection law

Michiel Rhoen
Leiden Law School, Leiden University, The Netherlands

Published on 31 Mar 2016 | DOI: 10.14763/2016.1.404

Abstract: As a result of datafication (the generation and acquisition of personal data from automated processes), consumers' activities generate large data streams. Analysis of these streams reduces privacy and shifts power towards data controllers. Consumers often contractually agree to this analysis of their data, but their autonomy can be questioned: the agreements often contain non-negotiable terms unilaterally drafted by data controllers. Consumer protection law can alleviate this power shift towards data controllers, but only if EU member states increase their enforcement efforts.

Keywords: Data protection, Consumer protection, Privacy, Big data

Article information

Received: 18 Dec 2015 **Reviewed:** 16 Feb 2016 **Published:** 31 Mar 2016

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-law

Citation: Rhoen, M. (2016). Beyond consent: improving data protection through consumer protection law. *Internet Policy Review, 5*(1). DOI: 10.14763/2016.1.404

This paper is part of 'Big data: big power shifts?', a Special issue of Internet Policy Review, supported by the Vodafone Institute for Society and Communications.

INTRODUCTION

Big data is shifting power away from consumers and data subjects towards data controllers. In a legal sense, natural persons often act as both a consumer and a data subject at the same time.[1]Controllers have come to collect data and metadata on an increasing number of common consumer activities like personal communications, online behaviour, shopping, banking and public transport – a trend known as datafication (Mayer-Schönberger & Cukier, 2013, p. 29). The Internet of Things (IoT) will soon generate even more data (ITU-T, p. 1). The collection and analysis of big data streams can amount to consumers' permanent surveillance. This gives

controllers the power to influence consumer behaviour through dynamic or discriminatory pricing, filter bubbles or subtly influencing individual decisions (nudging).

Big data's power shift has a significant privacy and data protection dimension. According to "Zimmermann's law",[2] this happens by virtue of technological progress alone (Malik, 2013). Data is also evolving into new currency. Increasingly, data controllers offer services like games and social networking not for money, but in exchange for the right to collect and use personal data. Consumers often enter these "privacy contracts" (Verhelst, 2012, Chapter 3) if they want to enjoy a service seemingly for free, but even paying customers are not safe from this practice (Perlroth, 2015). Nevertheless, the recently accepted General Data Protection Regulation (GDPR [PDF]) mentions consumer protection only once (Council of the European Union, 2016, p. 24 and note 1). Similarly, the European Commission's 2012 proposal for a consumer agenda mentions data protection efforts only in passing (2012a, pp. 3–4). The European Data Protection Supervisor, however, has stated that consumer protection law has a part to play in data protection, especially on the subject of transparency (2014, p. 2).

EU data protection law has facilitated the aforementioned power shift since the introduction of the 1995 Data Protection Directive (DPD).[3] It allows the collection and use of personal data based on consumers' consent, or if it is "necessary for the performance of a contract to which the data subject is a party". The GDPR contains a similar provision.[4] Compliance with the directive is then rewarded with the right to freely move this data within the European Union and to some other jurisdictions.[5]

These provisions seemingly empower data subjects, but data subjects acting as consumers lack effective participation options in the market (Rhoen, 2015, p. 65). They can hardly avoid privacy contracts: almost all banks, software and hardware vendors, social networking sites, digital content services, retail loyalty programmes and telecommunications providers employ them. The difficulties consumers face when invoking fundamental rights in court complicate matters further: privacy law does not clearly describe a minimum level of privacy that should always be maintained; instead, it provides criteria for the balancing of individual privacy against other interests. As a result, it does not offer simple rules for courts to decide cases. Claiming damages for privacy breaches is hampered by the fact that consumers "give it away in exchange for so little" (Schneier, 2015, Chapter 14).

If data controllers become too powerful, the validity of consumers' and data subjects' consent or their autonomy when entering into privacy contracts can be questioned. Therefore, controllers' increasing power should not remain unchecked. Analogous to the notion of *due process* in United States law, Gutwirth and De Hert have seen the application of three requirements that serve as checks on the unlimited exertion of power: participation, transparency and accountability (Citron, 2007, pp. 1256–1257; Gutwirth & de Hert, 2001, nos. 12–13). In western societies, many safeguards of fundamental rights at every level of government, for example the protection of suspects in criminal proceedings, can be "decomposed" into these three requirements.[6] Now that privacy contracts and datafication give private companies capabilities similar to those of police, prosecutors or national security agencies when it comes to data collection and use, these requirements and their effects on the underlying power dynamics have also become relevant in contractual relations.

Barnett and Duvall define power as "the production, in and through social relations, of effects that shape the capacities of actors to determine their circumstances and fate" (2005, pp. 39, 45–57). They refine the concept further by qualifying the expression of power (either through interaction or constitution) and the specificity of the social relations through which it works

(either direct or diffuse).[7] Using this conceptualisation of power, this contribution examines the following research question:

Can consumer protection law assist in attenuating the shift in power from consumers to data controllers caused by big data?

The following sub-questions will help to answer the research question:

- How does big data cause power to shift?

- Are data protection and privacy law effective in preventing this shift?

- What opportunities does EU consumer protection law offer for addressing the shift?

In answering the main question, this article considers only cases where a natural person is both a data subject and a consumer at the same time. The text references the final text of the GDPR unless otherwise specified.

HOW BIG DATA SHIFTS POWER TOWARDS DATA CONTROLLERS

Data controllers use their existing *structural power* over data subjects in the contracting phase to increase their *institutional power* after the contract is concluded. Structural power (expressed through constitution in direct social relations) follows directly from the roles actors play, i.e. the roles of suppliers and consumers in the market, and enables the powerful party to limit the capacity of the less powerful party to act in their own best interest. Institutional power (expressed through interaction in diffuse social relations) is the power differential resulting from "constraint(s) that human beings devise to share human interaction" (Barnett & Duvall, 2005, pp. 51–55; North, 1990, p. 4).

In the contracting phase, structural power expresses itself in the market as a lack of bargaining power on the consumer side, resulting in non-negotiable terms (*Océano Grupo Editorial SA v Roció Murciano Quintero and others*, 2000, para. 25). This reduces consumers' party autonomy and therefore touches on a key element of private law in Europe (Study Group on a European Civil Code & Research Group on EC Private Law (Acquis Group), 2009, p. 123). The root cause of this smaller bargaining power is asymmetric information. For consumers, the cost of information per contract is higher than it is for data controllers, mainly because the controllers unilaterally draft the privacy contracts and reuse them many times. This has led Gomez to state that the primary goal of consumer protection law is to overcome information asymmetries (2004, p. 193 ff; see also Slawson, 1970, p. 544). This higher cost of information, in turn, can be explained by analysing the dynamics of market participation (cf. Komesar, 2001, p. 30). The uneven distribution of the costs of information and organisation favours data controllers when consumers and controllers decide on contract terms. Individual consumers usually lack expertise and have little to gain by pooling their resources to negotiate a better deal on privacy in each separate contract.

Data controllers then use this structural power to increase their institutional power. As noted before, collection and use of personal data is lawful insofar as a data subject has consented to it, or if the processing is necessary for the performance of a contract. If the consumers' consent

allows for their permanent observation, the data controller has obtained a method of exerting power over the consumer (Bentham, 1787, p. Letter I; Schneier, 2014). Analysis and actual use of the data further increase this power. If the consumer has agreed to contract terms allowing it, the controller can then grant this power to third parties by using his right of free movement of data. Some of the largest of these third parties, data brokers, are not dealing with consumers directly; this makes the scale of the collection and use of their data less transparent to consumers (Federal Trade Commission, 2014, p. 46).

The increase in institutional power can express itself in many ways. Exposing a data subject to targeted advertising is an example of a subtle form of control: a data subjects' deeply personal characteristics can be gleaned from seemingly innocuous data. Such advertising is designed to appeal to personal desires which, although deeply and individually felt, are common to most people and therefore easily discovered (Packard & Miller, 2007, Chapter 7). The time frame and context in which these desires come into play in a consumer's life can become apparent by analysing data collected under privacy contracts and comparing it to previously determined patterns in a larger population (using "machine learning"). For example, a controller may determine whether someone is pregnant by observing a change in their buying patterns (Duhigg, 2012).

At least one possible effect of this increased institutional power is the further increase of data controllers' (already larger) structural power, for example, if loans to data subjects living in certain neighbourhoods only become available at discriminatory rates. In this way, the power shift could worsen the existing marginalisation of groups of people (Crawford & Schultz, 2014, pp. 99–101; Dwork & Mulligan, 2013, pp. 36–37).8Finally, the resulting power shift may allow controllers to leave consumers in the dark about the effectiveness of security measures against unlawful processing.

DATA AND PRIVACY PROTECTION LAW DO NOT PREVENT THE POWER SHIFT

EDRi (European Digital Rights), an EU-based advocacy group, asserts that the EU has a "strong, comprehensive and enforceable privacy protection framework"(EDRi, 2013, p. 1 [PDF]). This framework consists of EU data protection law (currently the Data Protection Directive, soon to be replaced by the GDPR), the Charter of Fundamental Rights of the European Union, national human rights law and the European Convention on Human Rights. Article 5(1) of the GDPR establishes a number of firmly worded principles governing the processing of personal data such as: lawfulness, fairness and transparency, purpose limitation, data minimisation, storage limitation and accountability. Article 6(1) limits the number of grounds for lawful processing. If performance of a contract depends on consent, article 7(4) stresses the need to carefully consider whether consent was freely given. Data subjects have the right not to be subjected to profiling (art. 21(1)). Controllers must use principles like "data protection by design and by default" (art. 25). And of course, the Strasbourg and Luxembourg courts guard over fundamental rights, including the right to privacy.

But the complex reality of both data protection and privacy law makes these legal protections less effective. Privacy as a human right is a complex issue because every case is different; the European Court of Human Rights in Strasbourg can only decide individual cases based on all relevant facts, in complex and long proceedings requiring expensive legal representation and

thus being not very accessible to individuals. Data protection law seems more easily applicable on its face, because it regulates data controllers' behaviour directly to ensure privacy (de Hert & Gutwirth, 2009, p. 44). But these formal requirements contain very complex standards aimed at specialised operators, intended to be enforced by specialised government agencies (Data Protection Authorities or DPAs). This is not necessarily a shortcoming of the GDPR: regulating controllers' behaviour is one way of keeping the GDPR enforceable, effective and relevant as technology progresses.

Even so, this complexity, combined with the increasing number of privacy contracts, makes consumer participation more difficult as it can make the effects of the GDPR unpredictable for consumers (Komesar, 2001, p. 28). A few examples:

- Fairness means that data is not collected in secret, that the purpose of the collection is made clear and that data subjects have access to their data (European Union, Agency for Fundamental Rights, European Court of Human Rights, & Council of Europe, 2014, p. 76). This requirement can improve transparency, but following it to the letter can in fact achieve quite the opposite effect. For example, if a controller provides exhaustive information and updates it several times a year, he effectively increases the cost of information (McDonald & Cranor, 2008). If the costs become too high, consumers may choose not to inform themselves.[9]

- Storage limitation only applies when identifiable data is kept on hand for "longer than is necessary" (art. 5(1)(e), GDPR). However, the drafter of a privacy contract can unilaterally define the purpose and the necessity. To discover what this principle means in a specific context, consumers need to carefully examine all contracts they enter, which they often do not (Bakos, Marotta-Wurgler, & Trossen, 2014, pp. 20-21, 31);

- Purpose limitation itself is limited: if a controller wants to reuse personal data previously collected for a different purpose, he "shall" take into account a number of complex factors, including the terms of the privacy contract itself (art. 6(4)(b));

- Opaque contextual parameters, such as "appropriate technical and organizational measures" determine the accountability of controllers and the "protection by design and by default" requirement (art. 24(1) and 25(1));

- Data protection impact assessments and data breach notifications should be carried out if there is a "high risk to the rights and freedoms of natural persons" (articles 34(1), 35(1)) but what constitutes a high risk is left undefined;

- Consumers enter into agreements and give consent in very simple or almost imperceivable ways. Ticking one of the ubiquitous "I agree" boxes on a website, and even the state of "technical settings for information society services", such as arcane browser or device settings can constitute consent (recital 32). The right to object to profiling may not apply in these cases (art. 21(1)).

- Finally, the complexity of data protection law encourages consumers to rely on enforcement by DPAs. But that DPAs fall short in enforcing existing data protection is apparently an "open secret" (Moerel, 2014, n. 110). If consumers are unaware that enforcement is lacking, this reduces transparency for consumers as well as accountability for controllers.

Another reason for privacy and data protection law's reduced effectiveness for privacy contracts is the fact that the ECHR was originally drafted to protect citizens against their governments in the aftermath of World War II. That the ECHR governs relations between citizens, including contractual relations, has been established in case law but states have a very wide margin of appreciation – wider than in cases against governments (Rhoen, 2015, p. 66). Whether the Charter of Fundamental Rights of the European Union applies to contractual relations seems doubtful at the moment (Frantziou, 2015, p. 671).

Finally, data protection and privacy are not the only fundamental rights recognised in Europe. Freedom of contract, party autonomy and freedom to conduct a business are also covered by fundamental rights.[10] A consumer's or controller's appeal on these rights may be used to make permanent observation through privacy contracts lawful. For example, if a consumer enters into a loyalty programme, he "performs" by allowing collection and analysis of personal data, whilst the controller performs by proposing "personalized offers" by him and "selected partners" according to art. 6(1)(b). Based on the term "personalized", a controller can arguably justify collecting data for as long as the contract exists, and on anything that can assist in further segmenting the market to further personalise his offerings. Common (and legal) business practices such as tying (offering two different contracts in one transaction, e.g. one for a "regular" service and another for the processing of personal data) further expand these possibilities.

In short, any practical effect of data and privacy protection law on the power shift associated with big data is reduced by the fact that both work through complex standards instead of simpler rules (Schlag, 1985, pp. 381-390). This complexity, together with the increasing number of privacy contracts, reduces transparency and the opportunities for participation for consumers as well as accountability for data controllers.

CONSUMER PROTECTION LAW CAN HELP SHIFT POWER FROM DATA COLLECTORS TO CONSUMERS

If a data subject is also a consumer, the European Union aims for a "high level of protection" of his economic activities.[11] The object of protection of consumer protection law is similar to that of data and privacy protection law: they both aim to protect the autonomy of the natural person (in the market for consumer protection; in a moral sense for data and privacy protection) (Gomez, 2004, p. 193 ff; Nissenbaum, 2009, p. 81-84). But the concept of protection for consumers is clearer. Where privacy and data protection law involve complex balancing of interests in an endless variety of contexts, consumer protection specifically aims to address power differentials based on information asymmetries in the market. Because of this specific applicability, applying EU consumer protection law to privacy contracts could help shift power back to consumers by improving participation and accountability. This follows from two features of EU consumer protection law: the scope of the fairness criterion and opportunities for participation.

Firstly, the scope of the fairness criterion is wider in consumer protection law than in data protection law. Applying consumer protection law would therefore increase the accountability of data controllers. This follows from the legal texts themselves.

The GDPR, as previously noted, mainly considers the processing of personal data unfair if it happens in secret or if profiling methods are faulty.[12] This is the basis for the GDPR's extensive disclosure requirements.[13] And indeed, mandatory disclosure is also an important regulatory technique in EU consumer protection law. But the resulting transparency is not enough to address substantive unfairness (Weatherill, 2013, p. 92-93). Therefore, in consumer protection law, fairness instead applies to the terms of the contract and to the way the consumer is persuaded to enter into it. The Unfair Terms Directive (UTD) regards a non-negotiated term in a contract or consent statement as unfair if "contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer."[14] This means that all rights and obligations are included in

establishing unfairness, not just those pertaining to the processing of personal data (*Commission des Clauses Abusives*, 2014; Wauters, Lievens, & Valcke, 2013, p. 64).[15] Furthermore, the Unfair Commercial Practices Directive considers a practice unfair if it is "contrary to the requirements of professional diligence and materially distorts or is likely materially to distort the economic behaviour of the average consumer with regard to the product."[16]

Admittedly, like the earlier examples from the GDPR, fairness in consumer protection law is also a complex standard. However, its application is easier for consumers because it relates to circumstances that they participate in every day. Furthermore, annexes to both the Unfair Terms Directive and the Unfair Commercial Practices Directive give concrete examples. Consumer advocacy groups have been giving guidance on their application, and taking offenders to court, since they came into force (Bultmann, 2008, no. 14; *Verbraucherzentrale Bundesverband*, 2013).

Applying consumer law's fairness criterion to privacy contracts can expand the accountability of data controllers when compared to only applying the GDPR. Consider the hypothetical case of a provider of a smartphone app enabling the user to use his camera flash LED as a flashlight (see Vincent Fleming, 2013). The provider could present an agreement in which he grants the consumer a license to use the app in return for which the consumer allows the provider, acting as a data controller, to collect location and usage data to provide advertising for as long as the app is installed.

In terms of data protection law, this case could arguably be made GDPR-compliant by presenting all the relevant clauses and obtaining agreement to them in exchange for a software license. Applying article 7(4) of the GDPR, containing a criterion for determining whether consent is freely given, may not improve matters for the consumer. Because the data collected is not one of the special categories of data as defined by article 9(1), explicit consent may be unnecessary. "Necessary for the performance of the contract" probably suffices to make the processing of personal data lawful, because the criterion of necessity is interpreted in the light of the clauses in the contract. Party autonomy dictates that consumers are free to perform their part by offering their personal data, even if this data is not necessary to turn a phone's LED on or off.

However, such a case would almost certainly violate art. 3, UTD. Allowing surveillance in exchange for the ability to switch an LED on or off seems like such a bad deal, that the "requirement of good faith" has probably not been met. Depending on how the app was advertised, offering the app under these conditions could also be called misleading according to article 6(1)(a) of the Unfair Commercial Practices Directive, insofar as it presents an offer with data protection relevance as a standard software license agreement – especially since consumers hardly ever read software licenses.

Secondly, consumer law offers better participation options than the GDPR when seeking a remedy in court or before an administrative authority. This is often burdensome for consumers, especially against an opponent with large resources (Galanter, 1974). Limited individual stakes in the outcome of costly proceedings may discourage him from bringing a matter to court. Article 11(1) of the Unfair Commercial Practices Directive and 7(2) of the Unfair Terms Directive state that EU member states "shall ensure" that consumer rights organisations can bring an action before the national courts. This allows consumers to pool resources, reducing the cost of information and participation; it also allows consumers to build on previous organisation efforts, reducing the cost of organisation. This improves the dynamics of participation for

consumers (Komesar, 2001, p. 30). The GDPR does not require member states to allow complaints by advocacy groups, it merely allows them to do so (art. 80(2)).[17]

A more indirect way in which consumer protection law offers better participation options stems from the treaties establishing the EU and the levels of harmonisation within the EU that follow from them. EU data protection law is based on conferral of competence by the member states, whereas consumer protection law is based on shared competence.[18] As a result, member states cannot increase the level of protection that EU data protection law provides unless it is expressly allowed, whereas for consumer protection law this is possible unless it is expressly forbidden (*Bodil Lindquist*, 2003, paras 96–67; European Commission, 2012b, pp. 5–6).[19] This can help consumers: for them, participation in legislation efforts is much harder at the EU level than at the national level (Rhoen, 2015, p. 65).

Thus, applying consumer protection law to privacy contracts can increase accountability for data controllers and offer better participation options for consumers. Both effects will decrease the institutional power of data controllers in favour of consumers.

CONCLUSION: IMPROVE ENFORCEMENT OF CONSUMER PROTECTION LAW

When compared to the GDPR, existing EU directives regarding unfair contract terms and unfair commercial practices can increase the accountability of data controllers and offer more effective participation options for consumers. This is important in addressing the increase in institutional power that data controllers stand to gain from big data.

However, this possibility can only materialise if consumer protection law is effectively enforced. Determining the effectiveness of the current enforcement regime is not easy, but in 2012 the Commission claimed that "(r)edress and enforcement mechanisms need to be further improved" and launched the European Consumer Agenda, partly to achieve this. The commission also identified perceived low individual stakes as one of the reasons why consumers often do not seek redress (European Commission, 2012a, sec. 3.4). Apparently, lack of effective enforcement and low individual stakes similarly affect the effectiveness of both consumer protection and data protection law. Under these circumstances, expecting beneficial effects from applying consumer protection law without increasing enforcement efforts can only lead to disappointment. Ensuring proper coordination between national and European authorities for data protection and consumer protection may also be needed. Having two or even more competent authorities in each member state on the subject of privacy contracts may not have any beneficial effect if this joint competence leads to indecision, turf wars or other intra-governmental inefficiencies.

At the same time, very strict enforcement has its own risks and limits. The power shifts associated with big data are too complicated to be addressed only by applying consumer protection law to privacy contracts. Yes, putting consumers under surveillance will become easier with time according to Zimmermann's law.[20] But big data is also driving important innovations and, in an important way, datafication is the price we pay for automation. Billing, correction of errors and malfunctions, and detection of hacking and crime all rely on data

generated by automated processes – "It's impossible to overstate the importance of logging" (Prevelakis & Spinellis, 2007). Any well-intentioned effort to suppress the creation, storage and analysis of event logs – in other words, to suppress datafication – could disempower both consumers and data controllers, as it takes away their opportunity to construct or counter evidence of mistakes or wrongdoing.[21] Data streams are also becoming a way of personal expression, e.g. in the "quantified self" movement, which means that curtailing their creation and use can interfere with yet another fundamental right (Nafus & Sherman, 2014). Addressing big data's power shifts by narrowly focusing on privacy contracts can cause unforeseen power shifts all by itself.

Nonetheless, spirited enforcement of consumer protection law for privacy contracts seems like the way forward. Both the Unfair Terms Directive and the Unfair Commercial Practices Directive offer open norms with ample possibilities to develop a nuanced approach. Controllers who necessarily have access to data streams on many aspects of consumers' lives, like banks and telecommunications providers, should probably be prevented from seducing consumers to allow permanent observation all too easily. On the other hand, consumers should have a reasonable amount of freedom to enter into contracts with providers of specialised data-intensive services. A nuanced approach has a lower risk of negatively affecting related fundamental rights and halting innovation, than blanket bans on the generation, storage and use of data. Of course, improving the enforcement of data protection law will also help.

Increasing enforcement efforts will certainly have a cost. Member states will have to provide additional funding; they also need to strengthen co-ordination between consumer- and data protection authorities, both at the national and the EU level. It may also be necessary to improve the dynamics of participation for consumers. For example, targeted subsidies for consumer and privacy advocacy groups at the national level, aimed at representation both in civil society and in court, could somewhat offset consumers' costs of information and organisation. This would complement similar subsidies at the EU level in member states that do not currently subsidise these efforts.[22]

But the benefits may very well outweigh the costs. The more consumers feel their privacy really is protected and enforceable, the faster industrialised societies can collectively benefit from datafication. Addressing the power shift associated with big data will therefore be an important part of Europe's economic future.

REFERENCES

Bakos, Y., Marotta-Wurgler, F., & Trossen, D. R. (2014). Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts. *Journal of Legal Studies, 43*(1). Retrieved from http://papers.ssrn.com/abstract=1443256

Barnett, M., & Duvall, R. (2005). Power in International Politics. *International Organization, 59*(1), 39–75.

Bentham, J. (1787). *Panopticon; or The Inspection-House, containing the idea of a new principle of construction applicable to any sort of establishment, in which persons of any description are to be kept under inspection, and in particular to penitentiary-houses, prisons, houses of industry, work-houses, poor-houses, lazarettos, manufactories, hospitals mad-houses and schools: with a plan of management adapted to the principle: in a series of letters, written in the year 1787, from Crecheff in White Russia to a friend in England*. Retrieved from http://cryptome.org/cartome/panopticon2.htm

Bodil Lindquist, No. C-101/01 (Court of Justice of the European Union, 6 November 2003). Retrieved from http://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=en

Bultmann, F. (2008, June). 30 Jahre Praxis der AGB-Verbandsklage: Kurzfassung des Gutachtens im Auftrag des Verbraucherzentrale Bundesverbandes. Verbraucherzentrale Bundesverband e.V. (vzbv). Retrieved from http://www.vzbv.de/sites/default/files/mediapics/kurzfassung_gutachten_verbandsklage_2008.pdf

Citron, D. K. (2007). Technological due process. *Wash. UL Rev., 85*, 1249.

Commission des Clauses Abusives. (2014, December 3). Recommandation n° 2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux. Commission des Clauses Abusives. Retrieved from http://www.clauses-abusives.fr/recom/14r02.htm

Committee on Legal Affairs and Human Rights, & Omtzigt, P. (2015). *Mass surveillance* (No. Doc. 13734). Strasbourg: Parliamentary Assembly, Council of Europe. Retrieved from http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=21583&lang=en

Council of the European Union. (2016, April 6). 5419/16: Position of the Council at first reading with a view to the adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

Crawford, K., & Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. *BCL Rev., 55*(1), 93–128.

de Hert, P., & Gutwirth, S. (2009). Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne, & S. Nouwt (Eds.), *Reinventing Data Protection?* (pp. 3–44). Springer Netherlands. Retrieved from http://link.springer.com.proxy.library.uu.nl/chapter/10.1007/978-1-4020-9498-9_1

Duhigg, C. (2012, February 19). How companies learn your secrets. *The New York Times*, p. MM30.

Dwork, C., & Mulligan, D. K. (2013). It's Not Privacy, and It's Not Fair. *Stanford Law Review Online, 66*, 35–40.

EDRi. (2013, April 10). EU: The global standard setter for privacy and data protection (EUDataP series, issue 2). EDRi. Retrieved from http://edri.org/files/eudatap-02.pdf

European Commission. (2016, March 23). Commission decisions on the adequacy of the protection of personal data in third countries. Retrieved 9 April 2016, from http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

European Commission. (2012a). *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and The Committee of the Regions: A European Consumer Agenda - Boosting Confidence And Growth* (No. COM(2012) 225 final). Brussels: European Union. Retrieved from http://ec.europa.eu/consumers/archive/strategy/docs/consumer_agenda_2012_en.pdf

European Commission. (2012b, January 25). 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). European Commission. Retrieved from http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

European Data Protection Supervisor. (2014, March 25). Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy. Retrieved from https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf

European Union, Agency for Fundamental Rights, European Court of Human Rights, & Council of Europe. (2014). *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union.

Federal Trade Commission. (2014). *Data Brokers: a call for transparency and accountability*. Retrieved from https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Frantziou, E. (2015). The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality. *European Law Journal, 21*(5), 657–679. http://doi.org/10.1111/eulj.12137

Galanter, M. (1974). Why the Haves Come out Ahead: Speculations on the Limits of Legal Change. *Law & Society Review, 9*, 95. http://doi.org/10.1.1.128.6122

Gomez, F. (2004). EC Consumer Protection Law and EC Competition Law: How related are they? A Law and Economics perspective. In H. Collins (Ed.), *The Forthcoming EC Directive on Unfair Commercial Practices - Contract, Consumer and Competition law implications* (pp. 187–208). The Hague: Kluwer Law International.

Gutwirth, S., & de Hert, P. (2001). Een theoretische onderbouw voor een legitiem strafproces. Reflecties over procesculturen, de doelstellingen van de straf, de plaats van het strafrecht en de rol van slachtoffers'. *Delikt & Delinkwent, 31*, 1048–1087.

ITU-T. (2012). *Overview of the Internet of things* (Recommendation No. ITU-T Y.4000/Y.2060). Geneva: International Telecommunication Union.

Komesar, N. K. (2001). *Law's Limits: The Rule of Law and the Supply and Demand of Rights*. Cambridge, UK; New York: Cambridge University Press.

Malik, O. (2013, August 11). Zimmermann's Law: PGP inventor and Silent Circle co-founder Phil Zimmermann on the surveillance society. Retrieved from http://gigaom.com/2013/08/11/zimmermanns-law-pgp-inventor-and-silent-circle-co-founder-phil-zimmermann-on-the-surveillance-society/

Mayer-Schönberger, V., & Cukier, K. (2013). The Rise of Big Data: How it's Changing the Way We Think about the World. *Foreign Affairs, 92*(May/June 2013), 28–40.

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society, 4*(3), 540–565.

Microsoft. (2016, January). Privacy Statement [Company website]. Retrieved 15 March 2016, from https://privacy.microsoft.com/en-us/privacystatement/?PrintView=true

Moerel, L. (2014). *Big data protection: how to make the draft EU regulation on data protection future proof. Oratie 14 februari 2014*. Tilburg: Tilburg University.

Nafus, D., & Sherman, J. (2014). This One Does Not Go Up To 11: The Quantified Self Movement as an Alternative Big Data Practice. *International Journal of Communication, 8*, 1784–1794.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, Calif: Stanford Law Books.

North, D. C. (1990). *Institutions, Institutional Change and Economic Performance*. Cambridge□; New York: Cambridge University Press.

Océano Grupo Editorial SA v Roció Murciano Quintero and others, No. ECLI:EU:C:2000:346 (Court of Justice of the European Union 27 June 2000). Retrieved from http://curia.europa.eu/juris/liste.jsf?num=C-240/98#

Packard, V., & Miller, M. C. (2007). *The Hidden Persuaders* (Reissue edition). Brooklyn, N.Y: Ig Publishing.

Perlroth, N. (2015, March 1). How Superfish's Security-Compromising Adware Came to Inhabit Lenovo's PCs. *The New York Times*. Retrieved from http://www.nytimes.com/2015/03/02/technology/how-superfishs-security-compromising-adware-came-to-inhabit-lenovos-pcs.html

Prevelakis, V., & Spinellis, D. (2007). The Athens Affair. *Spectrum, IEEE, 44*(7), 26–33. http://doi.org/10.1109/MSPEC.2007.376605

Rhoen, M. (2015). Big Data and Consumer Participation in Privacy Contracts: Deciding who

Decides on Privacy. *Utrecht Journal of International and European Law, 31*(80), 51–71. http://doi.org/10.5334/ujiel.cu

Schlag, P. (1985). Rules and Standards. *UCLA Law Review, 33*, 379.

Schneier, B. (2014, April). Metadata = Surveillance. *IEEE Security & Privacy, 12*(2). Retrieved from https://www.schneier.com/blog/archives/2014/03/metadata_survei.html

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (1st edition). New York, N.Y: W. W. Norton & Company.

Slawson, W. D. (1970). Standard Form Contracts and Democratic Control of Lawmaking Power. *Harvard Law Review, 84*, 529.

Study Group on a European Civil Code, & Research Group on EC Private Law (Acquis Group). (2009). *Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR). Outline Edition*. Munich: Sellier European Law Publishers.

Verbraucherzentrale Bundesverband. (2013, June 6). Samsung App-Store: Viele Klauseln unzulässig. Retrieved 10 April 2016, from http://www.vzbv.de/urteil/samsung-app-store-viele-klauseln-unzulaessig

Verhelst, E. W. (2012). *Recht doen aan privacyverklaringen: een juridische analyse van privacyverklaringen op internet*. Deventer: Kluwer.

Vincent Fleming, N. (2013, December 5). Sharing Your Location… In a Flash. Retrieved from https://www.consumer.ftc.gov/blog/sharing-your-location-flash

Wauters, E., Lievens, E., & Valcke, P. (2013). *A legal analysis of Terms of Use of Social Networking Sites, including a practical legal guide for users: 'Rights & obligations in a social media environment'* (EMSOC - User Empowerment in a Social Media Culture No. D1.2.4). Leuven: iMinds-ICRI. Retrieved from http://emsoc.be/wp-content/uploads/2013/12/D-1.2.4-A-legal-analysis-of-Terms-of-Use-of-Social-Networking-Sites-including-a-practical-legal-guide-for-users_Rights-obligations-in-a-social-media-environment6.pdf

Weatherill, S. (2013). *EU Consumer Law and Policy*. Cheltenham, UK: Edward Elgar Publishing.

FOOTNOTES

1. A consumer is "any natural person who is acting for purposes which are outside his trade, business or profession" (Art. 2(b), Directive 93/13/EC); a data subject is a natural person identifiable by personal data (Council of the European Union, 2016, p. 111).

2. "The natural flow of technology tends to move in the direction of making surveillance easier." (Malik, 2013).

3. Directive 95/46/EC of the European Parliament and of the Council 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.

4. Article 7(a) or (b), DPD; article 6(a) or (b), GDPR.

5. Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, United States and the Eastern Republic of Uruguay (European Commission, 2016).

6. For examples, see article 3(1) of the Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (Aarhus Convention); art. 8 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and artt. 6(3) and 13 of the European Convention on Human Rights.

7. Power is expressed through interaction if it results from what actors *do* (like drawing a gun during an argument); it is expressed through constitution if it results from what they *are* (like their authority or identity). Social relations are direct if parties to the relations are in *direct communication* with each other (like during negotiations); they are diffuse if their interaction happens as a result of *previously defined rules* (like when parties' behaviour is bound or prescribed by law) (examples from Barnett & Duvall, 2005, pp. 42–43).

8. Outside the scope of any privacy contract, data controllers can cooperate with governments to further national security interests in a "surveillance-industrial complex" (Committee on Legal Affairs and Human Rights & Omtzigt, 2015, p. 29).

9. As an example, Microsoft's privacy statement amounts to 35 pages and has been updated at least three times between June 2015 and January 2016 (Microsoft, 2016).

10. See articles 12, 16, Charter of Fundamental Rights of the EU.

11. Article 38, Charter of Fundamental Rights of the European Union.

12. See recitals 42 and 48 of the GDPR. For profiling, where it concerns the use of adequate mathematical or statistical procedures to prevent errors, data breaches or discriminatory effects, see recital 71.

13. See for example: art. 5(1)(b), art. 12(1, 3, 5) and art. 13(1-2).

14. Article 3, Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts ('Unfair Terms Directive'), OJ L 95, 21.4.1993, p. 29–34.

15. The first proposal for the GDPR contained a clause making consent invalid if there was a "significant imbalance between the position of the data subject and the controller" (art. 7(4)). The scope of the final provision is far more limited; specific consideration is only given to performance of a contract that is depending on consent.

16. Article 5(2) and 6(1)(a), Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149, 11.6.2005, p. 22–39

17. Nonetheless, the GDPR does require that member states allow these organisations to represent data subjects in individual proceedings, possibly lowering the cost of legal representation (art. 80(1)). Forum choice is handled equally for consumers and data subjects:

art. 79(2) of the GDPR allows data subjects to bring proceedings before a court in their country of residence, like art. 16(1), Regulation (EC) No 44/2001 does for consumers.

18. Article 39, Treaty on European Union (TEU); Article 2(f), 12, 16, 114 and 169, Treaty on the Functioning of the European Union (TFEU).

19. See art. 9(5), GDPR for an example where member states can increase the level of protection; See art. 8, 8a, UTD for an example of the greater freedom that consumer protection law allows. Recent EU consumer protection law tends to rule out this option. See art. 4, Consumer Rights Directive and art. 3(5), Unfair Commercial Practices Directive.

20. See footnote 2 above.

21. This is closely related to the "legitimate interest" ground for lawful processing of personal data (art. 6(1)(f), GDPR).

22. Art. 3(1)(b), European Parliament and Council Regulation (EU) No 254/2014 of 26 February 2014 on a multiannual consumer programme for the years 2014-20 and repealing Decision No 1926/2006/EC.