European Review of Private Law 5-2018 [635–660]

Ensuring Data Protection by Private Law Contract Monitoring: A Legal and Value-Based Approach*

Stéphanie van Gulijk** & Joris Hulstijn***

Abstract: Current legal frameworks for data protection are based on public law. They have a number of flaws. The notion of informed consent does not work in practice. Public legislation only covers the protection of personal data, but it doesn't cover data about groups and it doesn't cover conditions on usage of data for certain purposes. Moreover, in order to function in practice, businesses need to adopt these conditions as part of privacy policies and processes such as audits and impact assessments. Supervision by means of public entities is limited as regulatory agencies have little capacity. This gives private actors room for designing tools to protect their personal data. In this article, we will therefore suggest to utilize private law instruments for data protection. By incorporating conditions on usage of sensitive data in contracts and by setting up platforms for monitoring contract fulfilment, end users can be empowered to take enforcement into their own hands. We will propose a platform for assisting users in drafting contracts that take data protection into account, and for monitoring contract fulfilment. Feasibility of the proposal is illustrated by an application scenario, the sports tracker app.

Résumé: Les cadres juridiques actuels en matière de protection des données sont basés sur le droit public. Ils ont plusieurs inconvénients. La notion de 'consentement éclairé' ne fonctionnne pas dans la pratique. La législation de droit public couvre seulement la protection de données personnelles, mais ne couvre pas les données concernant des groupes et ne couvre pas non plus les conditions de l'usage de données dans certains buts. De plus, afin de fonctionner dans la pratique, les entreprises doivent adopter ces conditions comme faisant partie de politiques de protection de la vie privée et de méthodes telles que audits et évaluations d'impact. Le contrôle exercé par des organismes publics est limité car les agences de réglementation ont peu de pouvoirs. Ceci offre la possibilité aux acteurs privés de créer des outils permettant de protéger leurs données personnelles. Par conséquent nous proposons dans cet article d'utilizer des instruments de droit privé pour la protection des données. En incorporant des conditions concernant l'usage de données sensibles dans des contrats et en mettant en place des plateformes permettant de surveiller l'exécution du contrat, l'utilisateur final peut être habilité à se charger lui-même de l'exécution. Nous proposons une plateforme qui aide les utilisateurs à rédiger des contrats qui prennent en compte la protection des données et surveillent l'exécution du contrat. La faisabilité de la proposition est illustrée par un modèle d'application, l'application Sports Tracker.

* We would like to thank Mr.Dr. A. Berlee for her valuable comments to earlier versions of this article. The final version of this contribution was received on 12 July 2018.

** Professor in Private Law at Tilburg University, Tilburg Law School. Email: s.vangulijk@uvt.nl.

*** Assistant Professor Information Management at Tilburg University, Tilburg School of Economics and Management. Email: j.hulstijn@uvt.nl.

Zusammenfassung: Der derzeitige Rechtsrahmen für Datenschutz basiert auf dem öffentlichen Recht. Er hat eine Reihe von Mängeln. Das öffentliche Recht deckt nur den Schutz privater Daten ab, nicht aber den Schutz der Daten von Gruppen oder die Bedingungen für die Verwendung von Daten zu bestimmten Zwecken. Darüber hinaus müssen für ein Funktionieren in der Praxis Unternehmen diese Bedingungen als Teil der Datenschutzregelungen und Prozesse, wie Audits und Folgenabschätzungen, übernehmen. Die Überwachung durch staatliche Stellen ist begrenzt, da die Regulierungsstellen wenig Kapazitäten besitzen. Dies bietet privaten Akteuren Raum zur Gestaltung eigener Instrumente zum Schutz ihrer persönlichen Daten. Der vorliegende Beitrag schlägt die Nutzung von privatrechtlichen Instrumenten für den Datenschutz vor. Durch die Einbeziehung von besonderen Bedingungen für die Nutzung sensibler Daten in Verträgen und durch die Einführung von Plattformen zur Überwachung der Vertragseinhaltung werden Endnutzer in die Lage versetzt, die Durchsetzung des Datenschutzes in die eigene Hand zu nehmen. Die Autoren machen einen Vorschlag für eine Plattform zur Unterstützung von Nutzern bei der Erstellung von Datenschutzbedingungen einbeziehenden Verträgen und für die Überwachung der Vertragserfüllung. Die Machbarkeit des Vorschlages wird anhand eines Anwendungsbeispiel, der sports tracker App, illustriert.

Key words: Data Protection, GDPR, Contract Law, Privacy, Consumer Protection.

Mots clé: Protection des données, RGPD, Droit des contrats, Respect de la vie privée, Protection du consommateur.

Schlüsselbegriffe: Datenschutz, DSGVO (GDPR), Vertragsrecht, Privatssphäre, Verbraucherschutz

1. Introduction

1. Data drives modern society. The increasing availability of data and the increasing power of data analytics techniques, have driven up usage of personal data by large corporations and government agencies. In some cases, these trends mean that citizens' rights are being threatened. The current Facebook data scandal seems to open a new era in citizens' awareness of this threat. Citizens feel uninformed or even powerless towards these large organizations when consenting to new data practices.[1] When personal data is collected and processed, the rights of the individual are foremost protected by public legislation. Consider rights such as privacy,

1 L. Taylor, C. Richter, S. Jameson & C. Perez de Pulgar, *Customers, Users or Citizens? Inclusion, Spatial Data and Governance in the Smart City*, Maps4Society Final Project Report (University Of Amsterdam 2016), available at SSRN: http://ssrn.com/abstract=2792565; M.R. Berthold, *How to Intelligently Make Sense of Real Data* (Springer Verlag 2010); S. Van Gulijk & D. Op Heij, 'Oneigenlijk gebruik van data: een verkenning van privaatrechtelijke oplossingen', *WPNR (Weekblad voor Privaatrecht, Notariaat en Registratie)* 2016(7110), pp 453–458; A. McAfee & E. Brynjolfsson, 'Big Data: The Management Revolution', *Harvard Business Review* 2012(10), pp 3–9.

autonomy, fairness of decision making, protection of personal data,[2] or the right to be forgotten. Recently, the EU adopted the General Data Protection Regulation (Regulation (EU) 2016/679). The GDPR is applicable as from 25 May 2018 after a two-year transition period.[3] The aim of the GDPR is to reinforce data protection rights of individuals, facilitate the free flow of personal data in the digital single market and reduce administrative burden.[4]

2. However, in our opinion the GDPR has at least three flaws:

(1). The notion of informed consent, on which much legal doctrines to protect personal data are based seems ineffective.[5] In practice, contract terms on data protection are often hidden in complex sets of standard terms. Consumer tend to easily accept standard contract terms, regardless whether they really understand the consequences. Moreover, consumers often agree to the stated terms and conditions, because there is no real alternative.[6]

(2). Current public legislation only covers some of the many concerns that have been voiced. In particular, it focuses exclusively on the collection and processing of personal data, i.e. about individuals. Data concerning groups is not regulated.[7] Moreover, in this legislation there are few instruments to improve subjects' control over the way in which their data is being used.[8] Data practices like automated decision making (i.e. profiling) are covered by the GDPR, but the definition is very broad, and will likely be hard to enforce.[9]

---

2 Article 8 under 1, Charter of Fundamental Rights of the European Union (2000/C 364/01), www.europarl.europa.eu/charter/pdf/text_nl.pdf; A.S. Hartkamp, 'De invloed van het EU Handvest van de grondrechten op het privaatrecht', *WPNR* 2014/7035, p 961.

3 C. Tikkinen-Piri, A. Rohunen & J. Markkula, EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies, 34 *Computer Law and Security Review* 2018, pp 134–153; A. Freiherr von dem Bussche & A. Zeiter, 'Implementing the EU General Data Protection Regulation: A Business Perspective', 2. *European Data Protection Law Review* 2016, pp 576–581; B. Van Alsenoy, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation', 7. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 2016, pp 271–288.

4 GDPR, Introduction, under 2.

5 B.W. Schermer, B.H.M. Custers & S. van der Hof, 'The Crisis of Consent: how Stronger Legal Protection may Lead to Weaker Consent in Data Protection', 16. *Ethics and Information Technology* 2014, pp 171–182.

6 W.H. van Boom, I. Giesen & A.J. Verheij, *Gedrag en Privaatrecht, over gedragspresumpties en gedragseffecten bij privaatrechtelijk leerstukken* (Den Haag: Boom Juridische Uitgeverij 2008).

7 L. Taylor, L. Floridi & B. van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Dordrecht: Springer 2017).

8 A. Freiherr Von dem Bussche & A. Zeiter, 2. *European Data Protection Law Review* 2016, p 576.

9 See para. 14 of this article.

(3). Regulatory supervision of data protection frameworks is largely based on corporate compliance, embedded in a public law framework. Companies publish privacy policies, but compliance to these policies is hardly ever tested. In case of violations, often signalled by complaints from data subjects, regulators can only take action after the fact. Only in individual situations measures can be taken. Moreover, there seems not enough enforcement expertise and capacity to keep up with the scale of the challenges.[10]

3. How can we analyse these flaws? Consider the distinction between 'citizen' and 'consumer'. In the current public law framework, data subjects are seen as citizens. Their rights are generic and therefore relatively hard to enforce, because data practices vary across applications. Instead, data subjects can also be seen as consumers of a product or service. In the commercial domain, data are usually collected as part of a transaction or service provision relationship that proceeds according to a contract with terms and conditions. In that case, the appropriate framework appears to be private law. In their regulatory approach, public authorities are citizen-orientated. In private law, the notion of citizen is not being used. Mostly, private law distinguishes between non-professional and professional subjects. Non-professional users are referred to as consumers. Often consumers enter into contracts with professionals, who may have more power, or expertise. Professional contractors therefore have relatively more duties, for instance, to inform the consumer about the consequences of their decision.

4. In this article, we argue that private law instruments could in principle empower consumers to take data protection more into their own hands. The existing public law data protection framework remains valuable, but only as a 'last resort'. Private law, by contrast, is about what consumers themselves agree to. Given appropriate monitoring, better contract terms and conditions could empower consumers to take control over their personal data. However, currently consumers have limited and sometimes inappropriate private law remedies to respond to improper use of data about them. Moreover, the (pre)contractual duties to inform or warn are not well targeted for the use of personal data.[11]

5. What we see as the object to be regulated are 'data practices'[12]: re-occurring patterns of behaviour in which the collection, storage and usage of personal data, as well as the protocol for reaching agreement about the terms and conditions, are embedded. For instance, agreement needs to be reached about the purpose,

10 See for instance EAF (Andersson Elffers Felix), *Eindrapportage Organisatorische vertaling verordening en richtlijn gegevensbescherming* (Den Haag: Autoriteit Persoonsgegevens 2017).

11 S. Van Gulijk & D Op Heij, *WPNR* 2016/7110, pp 453–458.

12 L. Lessig, *Code: and Other Laws of Cyberspace* (New York: Basic Books 1999).

valuation of data as a counteroffer, and communication. Note that data practices are to a large part automated and are increasingly being standardized.

We see three reasons why private law instruments are particularly suitable for regulating emerging data practices.

6. First, let us consider purpose binding. The notion of purpose is already central to the current public law practice of data protection and remains central in the GDPR.[13] The idea is to minimize data collection, access rights and storage duration, unless it is collected for a specific purpose or further processing is not incompatible with that purpose.[14] Which data is really needed? In general, that question is open for interpretation. Now observe that usually the purpose for collecting and processing data is linked to the specific product or service that is being offered. In practice, the purpose will therefore be described in the form of a specific contract, so we do not have to rely on generic assumptions. Instead, the contract should specify what data may be collected and processed.

7. Second, what is the counter offer? The saying goes: 'Data is the new gold'.[15] If data can be converted into value, that leads to numerous possibilities. In many business models, consumers essentially pay for services by providing personal data. For example, platforms like Facebook make money by advertisements. In order to sell advertisements, the platforms need attention, measured as unique visitors. Attention is generated by content, which is provided by other users (holiday pictures; news feeds; links). If providing access to content is so essential for a business model, it should be properly paid for. Moreover, consumers should be able to negotiate terms and conditions on the usage of such content. Digital platforms therefore play an important role in discussions about protecting the privacy of consumers.[16]

8. Third, consumer empowerment is an important issue. Collectively, consumers do have power, because the business needs their data. Users may or may not grant access, but currently, users have no choice but to grant access if they wish to make use of the service.[17] Current privacy policies are one-size-fits-all. After the agreement is signed, the user becomes effectively powerless. Of course, withdrawal of

---

13 95/46/EC.

14 A. Freiherr von dem Bussche & A. Zeiter, 2. *European Data Protection Law Review* 2016, p 576.

15 N. Kroes, Opening Remarks, Press Conference on Open Data Strategy, Brussels, 12 December 2011.

16 V. Mak, 'Private Law Perspectives on Platform Services. Airbnb: Home Rentals Between AYOR and NIMBY', 5. *Journal of European Consumer and Market Law* 2016, pp 19-25; Proposal for a Directive on certain aspects concerning contracts for the online and other distance sales of goods, https://eur-lex.europa.eu/legal-content/ALL/?uri=COM:2015:0635:FIN; L. Graef, 'Het misbruikverbod op het internet; onlineplatforms als poortwachters van persoonsgegevens', *Computerrecht* 2014(38), pp 89-94.

17 B.W. Schermer et al., 16. *Ethics and Information Technology* 2014, pp 171-182.

consent is legally possible but the data can hardly be returned. This would improve if data are physically stored on a neutral platform, such as Hub of All Things or Databox,[18] that gives users control over data access. What if clauses about data protection in contracts become individually negotiable? Would this enable users to remain better in control?

9. So, there are at least three reasons why private law is in principle capable of playing a more central role in data protection. However, although private law instruments are relatively easy to adjust compared to public law, they need to be further developed to improve consumer data protection. There are fruitful analogies in this respect with the notion of informed consent in health care services,[19] and special duties for businesses in case of long term relationships.[20] The research question to be answered in this article is twofold:

What role could private law play in consumer data protection, and what technological tools are needed to support that role?

The remainder of the article is structured as follows. Section 2 details the concerns about current data practices. Section 3 provides some background on the current public and private law system of data protection, and why they are insufficient to deal with the challenges. Section 4 shows how private law instruments could be improved and be supported by a framework for contract negotiations and monitoring. Section 5 sketches an application scenario to show feasibility of the proposal. The article ends with conclusions and suggestions for future research.

2. Concerns About Data Protection Practices

10. It is clear that more data is available now, of more different types and about more different subjects, and that data is changing at a faster pace, than ever before. This idea of 'Big data' has been summarized by the three 'Vs': volume, variety, velocity.[21] Crucial is that more data is now actually being used for decision making. Much decision making is done automatically, as the tools and techniques of data analytics, business intelligence or data mining, are now powerful and mature enough to be applied at a large scale.[22] For instance, data mining tools can detect

18 Hub of All Things (hubofallthings.com), Databox, www.databoxproject.uk.

19 For collecting personal data in health care services the GDPR holds a stricter regime than for personal data in general. Instead of 'informed consent', 'explicit consent' is required. Arts 8 and 9 GDPR.

20 M.J. Becker, B.A.M. van Stokkom, P.J.M. van Tongeren & J.-P. Wils, *Lexicon van de ethiek* (Assen: Van Gorcum 2007); J.W. Berg, P.S. Appelbaum, C.W. Lidz & L.S. Parker, *Informed Consent: Legal Theory and Clinical Practice* (New York: Oxford University Press 2001).

21 A. McAfee & E. Brynjolfsson, *Harvard Business Review* 2012, pp 3–9.

22 H. Chen, R.H.L. Chiang & V.C. Storey, 'Business Intelligence and Analytics: From Big Data to Big Impact', *MIS Quarterly* 2012(36), pp 1165–1188.

patterns in data, which may be used for profiling.[23] As with the use of most technologies, data practices assume an implicit set of social values, which are not necessarily in line with the values of the stakeholders.[24] The increased scale of application, triggers concerns about the implicit social values of these data practices, and the rights of data subjects involved. In particular, peoples's privacy, autonomy, balance of power, and the fairness of decision making are at stake.

11. The right to *privacy* was historically about the 'right to be let alone'.[25] In modern legal practice, privacy protection in information has shifted to the more restricted notion of data protection. An illustrative case was the *Schrems* case in which the Court of Justice of the European Union (CJEU) repeated its position that the protection of the fundamental right to respect private life at EU level needs derogations and limitations in relation to the protection of personal data. This had to apply only in so far as is strictly necessary. Legislation permitting public authorities to have access on a generalized basis to the content of e-communication had to be regarded as compromising the essence of the fundamental right to respect for private life.[26] Yet there are more values than just privacy at stake.

12. Once data is shared it is out in the open and often beyond control of the person the data is about. What about individual *autonomy*? How can a subject ensure that data about him or her remain correct and complete? Under the previous data protection legislation and under the GDPR, data subjects have the right to rectification.[27] That means in practice that the controller of personal data needs a procedure that enables data subjects to file a request and have data corrected. Ultimately, a subject should also be able to withdraw from a service, and have all data removed. This is different from the right to be forgotten,[28] which has become widely known after the *Google/Spain* case.[29] In this case, the CJEU ruled that European citizens have a right to request that search engines, such as Google, should

---

23 See M. Hildebrandt, 'Defining Profiling: A New Type of Knowledge?' in: *Profiling the European Citizen: Cross-disciplinary Perspectives* (Springer 2008), pp 17-45.

24 M.J. van den Hoven, P.E. Vermaas & I. van de Poel (eds), *Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains* (Berlin: Springer 2005).

25 D.J. Glancy, 'The Invention of the Right to Privacy', *Arizona Law Review* 1979(21), pp 1-39; S.D. Warren & L.D. Brandeis, 'The Right to Privacy', *Harvard Law Review* 1890(4/5), pp 193-220; T. M. Cooley, *A Treatise on the Law of Torts, or, the Wrongs Which Arise Independent of Contract* (Callaghan 1888).

26 ECJ 6 October 2015, *Schrems*, curia.europa.eu/juris/liste.jsf?&num=C-362/14, paras 92-94. See also E. Kosta, *Surveilling Masses and Unveiling Human Rights – Uneasy Choices for the Strasbourg Court (Inaugural Address)* (Tilburg University 2017).

27 GDPR, Article 16.

28 B.J. Koops, 'Forgetting Footprints, Shunning Shadows: A Critical Analysis of the "Right to Be Forgotten" in Big Data Practice', 8. *SCRIPTed* 2011, pp 229-256.

29 ECJ 13 May 2014, *Google Spain SL, Google Inc.* v. *Agencia Española de Protección de Datos (es), Mario Costeja González*, curia.europa.eu/juris/liste.jsf?&num=C-131/12.

remove links to personal data that appear when you search for an individual's name when requested.[30] This is about information that appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine.[31] This case was important in the discussion about how to weigh freedom of speech and the right of the public to know about public figures,[32] against the right to privacy of the individual. Search engines must handle cases on an individual basis.[33] However, both the right to rectify and the right to erasure, presuppose that the data subject already knows what specific data have been collected about them, by whom, and for what purposes, and how the data is actually being used. Currently, subjects do not generally know these things.[34] This information-asymmetry also weakens their legal position, as the data subject has burden of proof to demonstrate a breach of data protection laws.[35]

13. Finally, there is the aspect of *balance of power.* Large data brokers such as Google, Apple, Amazon, Microsoft or Facebook have now collected such data sets about consumers, that they can quickly launch new products or services.[36] They have an enormous competitive advantage in the market for digital services. Access to huge amounts of data about consumer behaviour, concerning search, shopping, working life and leisure, makes these companies very powerful. Moreover, they control the platforms (Android, iOS, Microsoft) and devices (mobile phones, tablets, personal computers) which people use to gain access to digital services.[37] For many people, online platforms controlled by these giants have now become the main source of news stories.[38] Search engines and the internet have effectively

30 The links are not removed if you search for that information but not use the name of the person.

31 European Court of Justice, *Google Spain SL and Google Inc.* v. *Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 2014, Case C-131/12.

32 In the *Google/Spain* case not a public figure but a lawyer was at stake. On the discussion about free speech and privacy after Google / Spain see S. Kulk & F. Borgesius, '*Google Spain* v. *González*: Did the Court Forget About Freedom of Expression? Case C-131/12 Google Spain SL and *Google Inc.* v. *Agencia Española de Protección de Datos and Mario Costeja González*', 5. *European Journal of Risk Regulation,* 2014(3), pp 389-398.

33 For instance, Google writes a yearly report to justify the decisions about removal requests (transparencyreport.google.com).

34 Compare Art. 13 GDPR.

35 B. Van Alsenoy, 7. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 2016, pp 271-288.

36 N. Wolters Ruckert & L. van Sloten, 'Big Data: Big Privacy Challenges', *Tijdschrift voor Computerrecht,* 2016(3), p 82.

37 L. Graef, *Computerrecht* 2014, pp 89-94; V. Mak, 5. *Journal of European Consumer and Market Law* 2016, pp 19-25; Proposal for a Directive on certain aspects concerning contracts for the online and other distance sales of goods, https://eur-lex.europa.eu/legal-content/ALL/?uri=COM:2015:0635:FIN, p 6.

38 L. Taylor, C. Richter, S. Jameson & C. Perez de Pulgar, *Customers, Users or Citizens?.*

become a critical infrastructure on which modern economies depend.[39] Given the importance of such infrastructures, it is only natural that they are regulated.

14. Since big data is increasingly being used for decision making and these decisions are often made automatically, the *fairness of decision making* must be ensured. Fairness involves both equality and due process.[40] Fairness doesn't only affect the minority of subjects who want to 'opt out', as in the case of privacy, but it affects all those people who did agree to usage of their data, trusting that good use would be made of it. The GDPR prohibits profiling, at least in principle: 'The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.'[41] However, this definition covers any automated processing of data. It doesn't specify what is undesirable about profiling. For instance, profiling may be considered unfair, when a person is reduced to a set of features (a profile), and decisions are based on generalization about the profile, which may not be true for the individual case.[42]

Moreover, already in paragraph 2 of Article 22, the scope of the prohibition is limited. The prohibition does not apply when (1) the decision is necessary for performing a contract between data subject and data controller, or (2) is authorized by law, or (3) is based on the data subject's explicit consent. That means that this clause will be hard to enforce.

In addition, it is very hard for an individual to verify fairness of decision making. One aspect of fairness is equality. Assessing equality involves a comparison to others in a similar position, but individuals lack the data to make such comparisons.[43] Another aspect of fairness is due process.[44] Decisions must be motivated, for instance by policy rules and evidence. Now suppose the premium on someone's car insurance is increased because the company wrongly classified the neighbourhood as 'risky'. How would a subject find out? Several authors are therefore arguing for improved computational or algorithmic accountability.[45] The

---

39 M. DE KONING, 'Fair play en marktwerking in de privacygevoelige wereld van Big Data', *Computerrecht* 2016(83), pp 160–166; EDPS, *Preliminary Opinion of the EDPS – Privacy and Competitiveness in the Age of Big Data: Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy* European Data Protection Supervisor 2014).

40 M. HILDEBRANDT, in *Profiling the European Citizen: Cross-disciplinary Perspectives*, p 309.

41 GDPR, Art. 22.1.

42 M. HILDEBRANDT, in *Profiling the European Citizen: Cross-disciplinary Perspectives*, p 309.

43 Compare B. VAN ALSENOY, 7. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 2016, pp 271–288.

44 D.J. STEINBOCK, 'Data Matching, Data Mining, and Due Process', 40. *Georgia Law Review* 2005(1), pp 1–84.

45 N. DIAKOPOULOS, 'Accountability in Algorithmic Decision Making', 59. *Communicatins of the ACM* 2016, pp 56–62; H. NISSENBAUM, 'Computing and Accountability', *Communications of the ACM,* 1994/37; D.K. CITRON & F.A. PASQUALE, 'The Scored Society: Due Process for Automated

algorithms and rules that determine decision making should be made transparent. Algorithms leave traces and record the policy rules and evidence used in decision making, either for individuals or on aggregate (e.g. profiles; classes). In principle, such traces could be converted into a representation format that makes the decision understandable to consumers. Consider for instance a decision tree, annotated with the rules and data used, and the sources. Technically, this is possible, although not for all kinds of algorithms. For example, neural networks or genetic algorithms are hard to convert into such a human readable form. So eventually the demand for computational accountability will affect the choice of algorithm.

3. Current Data Protection in Public and Private Law

15. The diagnosis above triggers the question in what way the legal system can contribute to a safe harbour for people sharing their personal and individual data, who are facing the problems mentioned. First, we need to answer the question what public and private law instruments currently apply.

3.1. Public Law First

16. Current legal data protection largely relies on a public law system, enforced by national data protection authorities such as for example the Dutch Autoriteit Persoonsgegevens (AP). Mainly, informing, preventing, and maintaining are the AP's central responsibilities. Under the GDPR, the data protection authorities have been given more power to start investigating. Many of the existing principles of data protection from the 1995 EU Directive, and the various national implementations of that directive, have been strengthened in the GDPR. Also, the sanctions, e. g. maximum fines, have been increased.[46] Organizations have been made more responsible for data protection. The principle of data minimization (only collect what is needed for a specific purpose) remains one of the guiding principles.[47] However, the question which data is really needed for a specific purpose, is open to interpretation. Therefore, such issues should be addressed explicitly and up front, for example as part of a data protection policy. The slogan is: 'privacy by design'.[48] For every risky project, a company must work out what the privacy impact would

---

Predictions', 89. *Washington Law Review* 2014, pp 1-33, papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209.

46 For example, in case a data controller does not fulfill his obligations (such as the accountability principle), he may be fined 10 million Euro, or 2% of the annual revenues worldwide, if that amount is larger. In case a data controller violates the GDPR foundations or breaches the rights of data subjects, he may be fined by up to 20 million Euro, or 4% of the annual revenues worldwide.

47 A. Freiherr von dem Bussche & A. Zeiter, 2. *European Data Protection Law Review* 2016, p 577.

48 A. Cavoukian, 'Privacy by Design: The Definitive workshop. A foreword by Ann Cavoukian', 3. *Identity in the Information Society* 2010, pp 247-251; Recitals Art. 78 GDPR; Art. 25 GDPR.

be. In practice organizations will often have to conduct a privacy impact assessment (PIA),[49] in order to classify which data is considered sensitive, and how the data must be protected.[50] Moreover, organizations are now explicitly required to appoint a data protection officer, who is made responsible for establishing and carrying out the privacy policies.[51] The adoption of the GDPR has also created an increasing awareness of the importance of data protection.[52] What we observe is that in practice, companies that have to comply to the GDPR make use of an existing structure for corporate governance and internal controls, that is familiar from accounting and compliance reporting.[53] For example, accounting firms offer IT audit services, to assess whether adequate security measures to protect personal data are taken, and are effective. The main incentive for such investments appears to be the avoidance of reputation damages.[54]

17. Therefore, Data Protection Authorities will try to generate publicity. They educate the public, as well as the organizations concerned, and generally raise awareness.[55] Data Protection Authorities are tasked to monitor and enforce the GDPR.[56] However, unless a citizen files a complaint, normally the authority will have no reason to start investigating.[57] Moreover, there is a lack of enforcement capacity. For example, in the Netherlands, the AP has an annual budget of 8.1 million Euro, and a capacity of 72 FTE. In 2016, AP concluded 197 investigations, and handled 303 cases in a lightweight manner.[58] The growing size of the digital market in the Netherlands and the expected number of data protection breaches compared with the enforcement capacity, the regulatory capacity will not be enough to cover all possible breaches.[59] Crucially, the consumer or data subject plays little or no role in this public law and corporate compliance mechanism. A subject may file a complaint, but investigations take a long time, and by nature, generally regulators can only take action after the fact.[60]

---

49 Art. 35 GDPR.

50 R. Clarke, 'Privacy impact assessment: Its origins and development', *Computer Law and Security Review,* 2009/25, pp 123-135.

51 See Art. 37 GDPR for more specific conditions.

52 C. Tikkinen-Piri et al., 34. *Computer Law and Security Review* 2018, pp 134-153.

53 C. Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press 2008).

54 C. Tikkinen-Piri et al., 34. *Computer Law and Security Review* 2018, pp 134-153.

55 See e.g. Annual report AP 2016.

56 GDPR, Art. 57.

57 Authorities can do ex officio examination.

58 Annual report Autoriteit Persoonsgegevens 2016.

59 EAF (ANDERSSON ELFFERS FELIX), *Eindrapportage Organisatorische vertaling.*

60 See for instance Art. 35 GDPR.

3.2. Private Law Instruments

18. In European contract law practices, individual autonomy and freedom of contract are most important basic principles.[61] Entering into a contract requires free will and proper understanding of its content and the rights and obligations that stem from it. Contracts can only be binding when the notion of consent has been fulfilled and parties have a proper understanding of what the contract involves. This notion of consent becomes particularly relevant when consumer sign a contract with professional parties, so called business to consumer (B2C) contracts. Generally, these professional parties make use of standard contract terms. One of the great advantages of using standard contract terms in B2C contracts is that it saves time and transaction costs. After all, individuals no longer need to negotiate each separate contract clause and can rely on standard contract terms including clauses that have been strongly discussed by branch organizations earlier. The downside is that consumers who sign new contracts that refer to standard contract terms may be less careful and often will not thoughtfully take notice of the contract terms. In Dutch contract law, there is a vivid usage of standard contracts. Practice shows that standard contract terms (too) easily apply to B2C contracts, even if the individual consumer does not take proper notice of the standard contract terms and its content.[62]

19. As a result, consumers may not have proper understanding of what is involved in the contract. At that point, consideration comes at stake.[63] As we observed, big data is increasingly being used for decision making and these decisions are often made automatically. More and more, consumers do not only pay with money for the goods or services rendered, but they pay by other means. For example, the price that needs to be paid when installing a 'free' smart phone app is access to their location data, or free access to their personal data. Or users may be asked to contribute by writing a review, so providers can offer a reputation score. The question is whether contract parties, in particular consumers, are aware of the price that is to be paid for the service of the other party when entering into a B2C contract. Also note the move from a single transaction, to a repeated transaction or even a long-term commitment. Consideration on what data is being shared and during which period of time then becomes more and more important.

---

61 E.g. H. Beale, B. Fauvarque-Cosson, J. Rutgers, D. Tallon & S. Vogenauer, *Cases, Materials and Texts on Contract Law,* (Oxford: Hart Publishing 2010), pp 25 ff.

62 M.B.M. Loos, *Algemene voorwaarden* (Den Haag: Boom Juridische Uitgevers 2013); S. Van Gulijk & D. Op Heij, *WPNR* 2016, pp 453–458; J. Hijma, 'The Concept of Nullity', in C.G. Breedveld-de Voogd, A.G. Castermans, M.W. Knigge, T. van der Linden & H.A. ten Oever (eds), *BW Krant Jaarboek* (Wolters Kluwer 2016), pp 23–24.

63 In general see H. Beale, B. Fauvarque-Cosson, J. Rutgers, D. Tallon & S. Vogenauer, *Cases, Materials and Texts on Contract Law.*

20. Consider an example: consumers who use the Runkeeper app need to give access to their location data so that Runkeeper can track users during their exercise.[64] However, Runkeeper does not stop tracking users after the workout but keeps collecting location data when the training session has finished. This is a clear violation of the purpose binding principle. Generally, consumers are not aware of this practice. Even worse, Runkeeper has been found to transmit personal data to a third party, even when the app or handset was not in use. The Norwegian Consumer Council has lodged a complaint against Runkeeper with the Norwegian Data Protection Authority over breaches of data protection laws.[65]

21. From a private law perspective, one could question whether the notion of consideration was fulfilled in this case.[66] Basically, contractual consideration is what consumers need to pay for the promise of delivery. Normally, this will be something of value, for the most part money. Increasingly service providers or good suppliers ask for access to personal data in return for their service or good. In bulk the data is of value. The question is: how much is access to your personal data worth? Compared to professionals, consumers are in a disadvantageous position. After all, they mostly are not aware of the collective worth of their personal data, they are not fully aware of the fact that personal data is collected (and distributed) on such large scale, and they will have trouble knowing who exactly has access to their data across the internet. What exactly did they consent to? This raises questions: are the notions consent and consideration still fit for purpose when 'payment' with personal data instead of money is at stake?

22. Another concern with data practices is that, in contract law, specific rules on the collection or use of personal data do not yet exist. As a result, consumers' interests are not protected well. Generally, in commercial transactions professional parties apply standard contract terms to inform the other party on issues such as liability, remedies and so forth. When these standard contract terms are unfair to consumers they are not allowed. For instance, clauses in standard contract terms that exclude or limit damages in relation to consumers, or clauses in standard contract terms that force consumers to bring their dispute to a court of arbitration instead of the civil court, are deemed unfair as they lead to consumers being in a possible worse situation than professional contract parties. This is not allowed according to persistent European contract law.[67] However, there is no such protection regarding the unfair use of *personal data.* This is questionable as standard

64 See for a similar case Autoriteit Persoonsgegevens, *Nike beëindigt overtredingen hardloop-app*, Nieuwsbericht 2016/11/8.

65 Norwegian Consumer Council, *Complaint concerning the mobile phone app Runkeeper* (Oslo: Norwegian Data Protection Authority 2016).

66 B. Lubomirov, 'Persoonsgegevens betalen de rekening', *WPNR* 2018(7181), pp 151 ff.

67 See ECJ 27 June 2000, C-244/98 (Océano); ECJ 21 November 2002, C-473/00 (Cofidis); ECJ 26 October 2006, C-168/05 (Mostaza Claro), ECJ 4 June 2009, C-243/08 (Pannon).

contract terms frequently hold (hidden) clauses on the collection of personal data. The protection of one's *private life* is a fundamental right.[68] Shouldn't the fact that the protection of one's private life is that important to the legislator also lead to effective protection in private law, by strengthening the contractual position of consumers towards professional contract parties?

4. Strengthening Data Protection Rights

23. We propose to address these issues, first, by strengthening data protection rights as part of contract law, and second, by software tools and a data governance framework that should empower users to negotiate better contractual terms, monitor contract performance, and challenge the organization in case of an apparent breach of contract.

4.1. Strengthening Data Protection Rights as Part of Contract Law

24. Providing personal data has become more than just a return favour and is, from a collective perspective, of high value. An important issue that needs attention is the information-asymmetry about the usage of personal data in B2C contracts. Practice shows that parties entering a contract often lack information on what will happen with their personal data.[69] Multiple causes play a role: generally people are not fully aware of the big value of their data to the other party; clauses on using personal data are not part of the contract or somewhat hidden; service providers have a much stronger economic (monopoly) position than consumers; people are not aware that the collection of data is an ongoing process during the period of the contract; or they may think there is nothing to hide. A recent Dutch TNS Nipo report on privacy as trade shows that 36–48% of consumers indicate that more or better information on apps in the pre-contractual stage would raise their awareness regarding the (possible) exchange of their personal data.[70] Does contract law fall short in ensuring that, in a pre-contractual stage, information is provided on supplying personal data as an important performance condition resulting from the contract? A safety net of default rules for consumers, embedded in national contract law seems necessary.

---

68 Art. 8 EU Charter: '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.'

69 L.B.A. Tigelaar, 'Sancties en doelstellingen van Europese informatieplichten', *NTBR* 2015(31), pp 206–213; M.B.M. Loos & J.A. Luzak, 'De nieuwe Richtlijn consumentenrechten', *Tijdschrift voor Consumentenrecht en Handelspraktijken* 2011(5), pp 184–191; A.L.M. Keirse, S.A. Kruisinga & M. Y. Schaub, 'Nieuws uit Europa: Twee nieuwe wetgevingsinstrumenten: de Richtlijn Consumentenrechten en het gemeenschappelijk Europees kooprecht', 1. *Contracteren: tijdschrift voor de contractspraktijk* 2012, pp 11-26

70 TNS Nipo, *Privacy als ruilmiddel: onvermijdelijk maar ook acceptabel?* (TNS Nipo 2016).

25. As we have seen, many services that consumers sign up for, such as the services provided by apps like Runkeeper, Whatsapp, etc, concern long-term relationships. This is evidently different from a sale of goods contract, which only involves a short-term relationship between seller and buyer. When it comes to long-term relationships, with no anticipated end of the affairs, default rules on personal data usage seem appropriate. Usually, the interests of parties engaging in long-term relationships are diverse and the balance of power plays a crucial role.[71] In this respect, in the early eighties of the twentieth century, Macneil argued that current contract law rules are not fit for economic reality in complex relationships. One of the underlying arguments he used was that contract law presumes that people close simple deals, such as buying and selling a good (discrete transactions). This presumption, on which contract law is founded, conflicts with the practice of more complex agreements that involve long-term relationships. One of the main problems is the inability of contract parties to evaluate (future) risks.[72] When sharing one's personal data is part of the contract, this also holds uncertain future risks for consumers. Similar to earlier developments to protect consumers in the field of loan or stock agreements, specific duties of care regarding sharing personal data should be required in contract law.

26. One could also argue that the way one's personal data is dealt with should be an explicit term in a contract or in standard contract terms. In Dutch contract law, freedom of contract is the basic principle. It allows parties to provide the terms and conditions that will govern the relationship. Even if the contract brings along legal effects that benefit one party more than the other, it is allowed. Only if contractual arrangements are against mandatory law, local customs or public order, contractual freedom is restricted. In Dutch contract law, the iustum pretium theory was rejected in the past, in favour of contractual freedom. This theory brings along that contractual arrangements should be of equal value. In common law countries, the iustum pretium theory is leading, empowering judges to consider the equilibrium of the arrangements made.[73] In Dutch contract law however, contract parties freely determine the equilibrium between their contractual arrangements. Since consumers are in a weaker position than professional contractors, there is reason to protect them in case their personal data is at stake. Although the iustum pretium theory is not leading in Dutch contract law, a fair balance between data protection of individuals and commercial interests of the other party should be strived for.

---

71 M.W. DE HOON, 'Effective Unilateral Ending of Complex Long-term Contracts', 19. *ERPL* 2005, pp 469-490.

72 I.R. MACNEIL, *The New Social Contract: An Inquiry into Modern Contractual Relation,* (New Haven: Yale University Press 1980); I.R. MACNEIL, 'Reflections on Relational Contract Theory after a Neo-Classical Seminar', in D. Campbell, H. Collins & J. Wightman (eds), *Implicit Dimensions of Contract: Discrete, Relational and Network Contracts* (Oxford: Hart Publishing 2003), pp 207-218.

73 J. HALLEBEEK, 'De iustum pretium-leer en het evenredigheidsbeginsel', *Ars Aequi* 1969(1), pp 59-64.

Especially where it concerns consumers (not being repeat players). On other issues, such as liability limitation, clear legal protection has already been established in the benefit of consumers. What about data protection?

4.2. Software Tools and a Data Governance Framework

27. Users and organizations must formulate contracts, which state precisely which data are collected, for which purpose, and against which compensation. Such contracts should be electronically represented and automatically enforceable. Therefore, they may be called *smart contracts.*[74] The general idea of smart contracts was first introduced by Szabo,[75] motivated by the hope that a formal contract could reduce disputes and misunderstanding. Smart contracts have gained more popularity with the rise of block-chain technology, which makes it possible to securely store the terms and conditions of a contract.[76] Recent papers about this topic do not only address the technical aspects of smart contracts, but also deal with legal aspects.[77]

The components of Figure 1 (see below) are typical for a system that implements smart contracts.[78] For instance, Idelberger et al.[79] discuss a system design to support the following contractual activities: (1) formation and negotiation, (2) contract storage and notarizing, (3) enforcement and monitoring, (4) modification, and (5) dispute resolution. In our design of Figure 1, modification and dispute resolution are not separate functions, but are taken to be part of the 'challenge and response' functionality. However, a difference is that online dispute resolution typically involves some trusted external party (mediator). Here the platform offering the contract monitoring tools, will also partly fulfill that role.

28. Furthermore, the data infrastructure must monitor the way data is actually being used and provide frequent reports: *contract monitoring.* For example, in case of a

---

74 T.F.E. Tjong Tjin Tai, 'Smart contracts en het recht', *Nederlands Juristenblad* 2017(146), pp 176–182, en 'Juridische aspecten van blockhain en smart contracts', *TPR (Tijdschrift voor privaatrecht)* 2017, p 563.

75 N. Szabo, *The Idea of Smart Contracts*, Research Note, 1997, archive.org/details/perma_cc_V6AZ-7V8W.

76 D. Magazzeni, P. McBurney & W. Nash, 'Validation and Verification of Smart Contracts: A Research Agenda', 50. *Computer* 2017, pp 50–57.

77 M. Raskin, 'The Law and Legality of Smart Contracts', ssrn.com/abstract=2959166; A. Savelyev, 'Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law', ssrn.com/abstract=2885241.

78 G. Governatori, 'Representing Business Contracts in RuleML', 14. *International Journal of Cooperative Information Systems* 2005, pp 181–216; G. Governatori & A. Rotolo, 'Norm Compliance in Business Process Modeling', in M. Dean (ed.), *RuleML 2010* (Springer Verlag 2011); *L 2016*, pp 167–183; G.F. Governatori, Idelberger, R. Riveret & G. Sartor, 'On Legal Contracts, Imperative and Declarative Smart Contracts and Blockchain Systems', *Artificial Intelligence and Law* Online First, March 2018, DOI org/10.1007/s10506-018-9223-3.

79 F. Idelberger, G. Governatori, R. Riveret & G. Sartor, 'Evaluation of Logic-Based Smart Contracts for Blockchain Systems', in *Rule-ML* (2016), pp 167–183.

Sportstracker App, the infrastructure would report that GPS location data is collected for a certain period, and subsequently that these data are used to calculate 'personal bests' for a certain route, and that these personal bests are shared among users. These reports may take the shape of a dashboard with graphical representations of the key indicators.[80] Using these reports, stakeholders like users and regulators can determine whether the organizations actually conform. If not, users can organize themselves and take immediate action: raise awareness, (threaten to) withdraw consent, or negotiate a better compensation. Note that already processors have an obligation to keep records of all processing activities.[81] However, in current practice, documentation is treated as a generic obligation; at the same level as the one-size-fits-all privacy policy. What we propose is to monitor and report what happens with individual data.

The expectation is that if the data infrastructure and contract negotiating, monitoring and enforcement tools are embedded in the right governance structure, they could empower data subjects and provide them with more autonomy and control over their data. In particular, the party hosting the data infrastructure and contract monitoring tools, should be independent of the parties that make use of the data for commercial services (see below). This may solve the information-asymmetry between the consumer and the professional party, alluded to above.

To understand the role that such software tools would play, we can use the metaphor of an electronic butler, who would 'negotiate privacy protections on our behalf'. The idea is suggested by Lessig,[82] and discussed at length by Schwartz.[83] Lessig observes that 'no one has the time or patience to read through cumbersome documents describing obscure rules for controlling data'. So instead of legal text we should have 'code', i.e. software systems, to do the reading for us. This is in line with Lessig's general conception of the regulation of cyberspace that stresses the importance of 'code'. Code is more than the text of legislation; code consists of the laws, market forces, architectural considerations, and social norms taken together, as implemented in actual software. [84]

29. There are signs that indicate that such a set-up is feasible in current circumstances. In the field of e-commerce, electronic intermediaries are well established.[85] They connect supply and demand, for instance in jobs or services. Such intermediaries also provide standard contracts or provide a communication

80 J.R. Kuhn & S.G. Sutton, 'Continuous Auditing in ERP System Environments: The Current State and Future Directions', *Journal of Information Systems* 2010(14), pp 91–111.

81 GDPR Art. 13.

82 L. Lessig, *Code: and Other Laws of Cyberspace*, p 160.

83 P.M. Schwartz, 'Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control and Fair Information Practices', *Wisconsin Law Review* 2000(4), pp 743–788.

84 L. Lessig, *Code Version 2* (New York: Basic Books 2006), p 123.

85 P.A. Pavlou & D. Gefen, 'Building Effective Online Marketplaces with Institution-Based Trust', 15. *Information Systems Research* 2004, pp 37–59.

procedure to help negotiate a contract for a job or service. Usually, such an intermediary also creates a community of users. When users in a community would organize themselves, they can establish trust and leverage their collective power, for example to ensure reliability of the service. Or consider the initiative of civic trusts: an emerging project that will apply the legal model of financial trusts to data management, building ownership and trust into the data governance infrastructure itself.[86] In this way, consumers could reinforce their contractual position in advance, before the contract is signed and personal data is shared. However, it appears to be an open question how to negotiate, implement and enforce such trusts in individual cases.

30. Suppose we would set up such an electronic infrastructure for contract negotiation and enforcement. What is needed in terms of software support and environment?

1. A framework to help users negotiate sensible contracts that take data collection and usage into account.
2. A data infrastructure with built-in mechanisms for monitoring adherence to these terms and conditions.
3. A governance structure with opportunities for challenging the organization, assessing the response, and passing judgment.

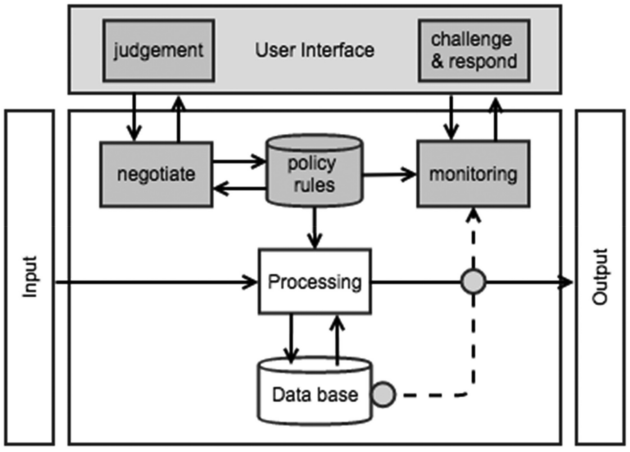

Figure 1. Design of an Electronic Infrastructure for Contract Negotiation and Monitoring

Figure 1 sketches a possible design for such a system. The design is based on a generic design that applies to any information system: input, processing, database

86 S.M. McDonald, *Toward (a) Civic Trust* (New York: Civic Hall (Collaborative Innovation Center) 2015).

for data storage and retrieval, and output. The components that need to be added are shown in grey.

1. A *negotiation component* would help users negotiate better and more transparent terms and conditions. Moreover, these terms and conditions should be formulated in such a way, that they can be effectively represented, measured and enforced. That means that specific key performance indicators must be agreed on for monitoring.
2. The result of the negotiation is a set of *policy rules* that regulate which data may be collected, how data may be used, how it is valued and how services are being paid for. So essentially, the policy rules form a kind of smart contract (see below).
3. A *monitoring component* collects and stores evidence about data practices, as they are conducted. This is shown in the diagram by a circle (sensor) which collects evidence about storage and retrieval in the database, and about processing output. The monitoring component continuously tests adherence to the smart contract, and helps to enforce it. For instance, it could trigger warnings, or automatically block data usage, after a violation.
4. The user interface allows the user to *challenge* the service provider: send a warning or ultimatum, (temporarily) block access to certain data, or ultimately, withdraw from the contract. Such challenges will surely trigger a *response.* The system should facilitate such a dialogue and log the interaction, as possible evidence for later.
5. After a certain period, agreed in the contract, the user passes *judgment.* He or she will weigh the benefits and efforts, and decide to continue, re-negotiate or end the contract. Also this function is supported by the user interface.

All components are connected to a user interface that should make these services both useful in practice, and easy to use. For instance, we envision a graphical representation for policy rules, and a clear indication of violations.

31. Concerning *governance,* this kind of proposal only makes sense when there is an independent party that hosts the data infrastructure, and contract negotiation and monitoring software tools. A clear governance structure is needed with specific roles and responsibilities, compare.[87] Only in this way, reliability of the contract monitoring can be ensured. There are several examples of projects and start-ups

87 M. Pascalev, 'Privacy Exchanges: Restoring Consent in Privacy Self-management', 19. *Ethics and Information Technology* 2017, pp 39-48.

that show the feasibility of a different data architecture, one where data streams are indeed stored and controlled on a neutral platform. Consider MIT's Personal Data Store,[88] the Databox project,[89] or the Hub of all Things project at Warwich University[90]: In these cases, commercial data brokers need a kind of 'lease' to get temporary access to data streams. However, when the data infrastructure and contract monitoring tools would be hosted by a dominant service provider, by the party controlling mobile devices, or by a data broker, it is clear that there is no balance of power. In that case, it will take additional effort to verify reliability and trustworthiness of the platform. For instance, users could ask for a trusted third party (IT auditor) to review reliability of the platform software and the procedures of the data controller.[91] Collectively, users do have the power that demand such transparency, if only they would organize. How users could organize is another topic that is out of scope for this article.

5. Illustration: The Sport Trackers App

32. To show the relevance and possible effects of the approach explained in Section 4, we will consider a simple example, a sports tracker app, to show that a negotiation and monitoring framework based on smart contracts, is both technically and legally feasible. The example is fictitious and simplified for explanatory purposes, but all elements are based on existing location-based services.[92]

Based on this example we will discuss possible properties for a contract that involves data sharing. These properties will be related to emerging theory on value-co creation.

5.1. Distribution of Data and Appropriate Business Model

33. There are several stakeholders, such as the party operating the sports tracker, the user, advertisers and other users in a community, maintained by digital platforms or social media. In order to make this app operative but also

88 Y.-A. de Montjoye, E. Shmueli, S.S. Wang & A.S. Pentland, 'openPDS: Protecting the Privacy of Metadata through SafeAnswers', 9. *PLoS ONE* 2014(7), doi.org/10.1371/journal.pone.0098790.

89 A. Crabtree et al., 'Building Accountability into the Internet of Things: The IoT Databox Model', *Journal of Reliable Intelligent Environments*. 2018/4/1, pp 39-55.

90 hubofallthings.com/.

91 See for instance for an overview: P. Balboni, *Trustmarks: Third-party Liability of Trustmark Organisations in Europe,* Msc Thesis (Tilburg University 2008).

92 See e.g. S. Dhar & U. Varshney, 'Challenges and Business Models for Mobile Location-Based Services and Advertising', 54. *Communications of the ACM* 2011, pp 121-128; D. Grewal, Y. Bart, M. Spann & P.P. Zubcsek, 'Mobile Advertising: A Framework and Research Agenda', 34. *Journal of Interactive Marketing* 2016, pp 3-14.

valuable, the tracker party will wish to collect certain data, such as the user's personal data (name, address, telephone number, age, gender), GPS tracking data of the user (location and time), sports related data of the user (sporting habits, personal standards, average speed), community related data of the user (posts on forum, likes, number of followers), and the number of views per advertisement, per user, per category etc. The sports tracker app has the following business model: it provides advertising space to advertisers, who want to target a specific audience. Advertising space is counted based on a formula that involves the number of individual viewers, the category of viewers, and the number and duration of views per period. To attract new viewers and to make viewers return, the sports tracker provides tracking functionality. This means that the route, duration and elevation of a training course are tracked, and shown to the user (on a map; in a graph). The tracker offers additional services, such as training advice, a personal record list for frequent routes, and comparisons of routes and records with other people training in the same neighbourhood. Finally, there are peripheral services, such as links to sports websites, shops for clothing and specialized gear, and a discussion forum. The aim is to sustain a community of practice and give people further reasons to increase viewing time and frequency. Based on generic data about users and actual browsing behaviour, a profile can be calculated that predicts how 'valuable' a specific user is as a potential customer in a marketing segment.

34. Figure 2 shows a diagram of the services that are being exchanged. The diagram makes use of the e3-value notation for business models.[93] In software development, such graphical models are intended to create an explicit and shared understanding of a business proposition, which can be understood by both business experts and programmers. In the diagram blue arrows indicate the transfer of objects or services of a certain value between parties. By means of ellipses, value transfers are grouped into transactions: one value transfer may only take place, if the counter transfer also takes place, earlier or later. Value transfers are linked by dashed lines, which eventually connect a need (red dot) with resources (circled red dot). Value models highlight that in many cases, value is created in a network of organizations. In other words, they highlight the notion of value co-creation.[94]

93 J. Gordijn & J.M. Akkermans, 'Value-based Requirements Engineering: Exploring Innovative E-commerce Ideas', 8. *Requirements Engineering* 2003, pp 114-134.

94 C. Grönroos & P.J. Voima, 'Critical Service Logic: Making Sense of Value Creation and Co-creation', 41. *Journal of the Academy of Marketing Science* 2013, pp 133-150.

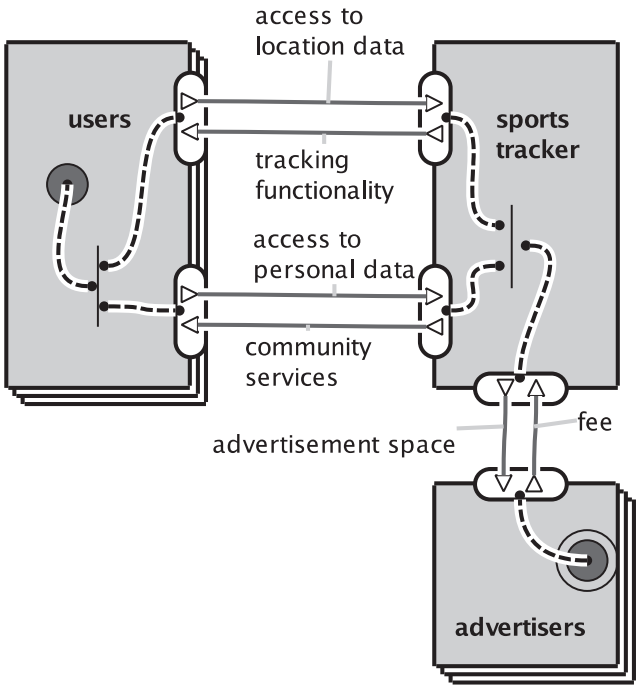

Figure 2 Value Model of the Sports Tracking Application

5.2. Reciprocity and Transparency

35. Depending on how much data the tracking partner wishes to collect and use, the trackers' service could vary. Generally, a contract is based on a service offered at several distinct service levels. Basic services can only be offered when access is given to basic data; more advanced services may be provided in return for access to more data, more sensitive data, or the right to share the data wider. This idea of reciprocity underlies most forms of transactions. It also gives rather detailed insights to consumers in the collection and use of data. This provides them with essential information. In term of rationality, this will empower consumers, as they will have more autonomy as to the personal data they are willing to share, and for which purpose. For example, the app user can decide whether or not he will provide:

- Access to location data [Y/N]
- Access to specific personal data (name, address, preferred sport) [Y/N]
- Right to share aggregated data in community (anonymous) [Y/N]
- Right to share sports related data in community (traceable) [Y/N]
- Contributions to community [text]

Depending on the user's consent to share above data, the tracker may provide:

- Tracker functionality, only if user provides access to location data
- Competitions and rankings, only if user provides access to location and personal data, and allows tracker to share aggregated location data with other users (anonymous)
- Community services, only if user provides access to location, personal data, and contributions, and allows tracker to share data with other users (traceable)

36. So, in this example, we distinguish three service levels, in which the exchange of access to data for services can be seen as *reciprocal*: basic level, anonymous sharing, and traceable sharing. In general: the more someone is willing to invest in the service, in terms of time, efforts and access to data, the more they receive in terms of service levels.

Another desirable property of this type of contract is *transparency*: it is clear what is being offered in return for what. It shows for instance that access to data is treated as a counter offer. Moreover, it provides clear definitions of acceptable behaviour. Clear performance indicators can be derived, to facilitate monitoring and possible redress, as discussed above.

37. Like most contracts that regulate services, contracts can be *renewed.* The decision to renew a sports tracker contract is the proper moment to evaluate and judge the behaviour of the service provider. In principle, a user could decide to terminate the contract, re-negotiate, or continue the current services. By having contracts not automatically renewed, users are made aware that they do have a choice. This may empower users and restore their autonomy to enter into a contract based on informed consent about the content of this contract.

Summarizing, what we propose is a set of tools for contract negotiation and monitoring that allow *layered consent*: users may accept or refuse collection, usage and distribution of specific types of data, in return for specific services.

6. Conclusions and Discussion

38. In this paper, we have argued that, in addition to public law initiatives on data protection, such as the GDPR, private law instruments and software tools could empower consumers to take data protection more into their own hands. Private law enables consumers to take control in their relationship with professional parties wanting to use their personal data. This is required since the possible remedies to invoke by a consumer whose data is being used improperly, currently seem insufficient. In relation to professional parties, consumers have limited and sometimes inappropriate remedies to respond to improper use of data about them. Existing

(pre)contractual duties to inform or warn are not well targeted for the use of personal data.[95]

39. We discussed three main reasons why private law instruments are particularly suitable for regulating emerging data practices: purpose binding as a central concept in data protection, professional parties counter offering services in return for consumers sharing access to personal data, and consumer empowerment after the agreement is signed. Consider the following scenario. An organization formulates a data policy. The policy clearly states which data are collected, for which purpose, and against which compensation. Some trusted infrastructure monitors the way data is actually being used and provides frequent reports, for example through a dashboard. Using these reports, consumers or representatives of consumers can determine whether organizations conform to the policies. If not, they can take action. Besides private law, technological support may be needed for such empowerment. We formulated the following research question: Which legal instruments does private law already provide for consumer data protection, and which legal instruments or technological support would be needed to could be added relatively easily?

The proposal is partly motivated by Lessig,[96] who shows that not all regulation is conducted by legislation alone. Lessig's famous slogan 'code is law' refers to the fact that many rules and regulations are adopted at a local level, as part of systems and processes in organizations and platforms. It is at this local level, that private law seems more effective as a legal instrument, as it is closer to the actual practice of allow access to collect data for a purpose.

In Sections 2 and 3, we have explored legal instruments to protect data. In particular, we argued that private law instruments, mainly stemming from contract law, are not sufficient in protection personal data in B2C contracts. Autonomy and consideration are important principles in European contract law but in practice they seem to fall short in data protection. Therefore, consumers, in particular users of services offered by mobile apps, need to be strengthened in their rights to freely enter into (or withdraw from) a contract in which sharing one's personal data is one of the most important contractual agreements.

In Section 4, we discussed one of the possible ways to improve the regulation of data practices: by means of software tools. Tools can be developed to help users and service providers negotiate better contracts, monitor and record evidence of adherence to the contract, and if needed, help users challenge the service provider, and enforce the contract. Smart contracting is an interesting development in this respect. Basically, it enables the user and provider of apps to make better informed choices. It has many possible advantages, such as transparency to all

95 S. Van Gulijk & D. Op Heij, *WPNR* 2016, pp 453-458.

96 L. Lessig, *Code Version 2*, p 123.

parties involved, automated processing of the choices made, fixed service provision in advance, clearance as to where the data flows to. However, some of the main challenges of smart contracting are contract monitoring and finding an appropriate governance structure.

In Section 5 we presented an illustrative case, a sports tracker app, to explain how these software tools could work in practice. We presented a value model and an example contract that distinguishes three service levels: basic level, anonymous sharing, and traceable sharing. Depending on which service level is agreed, the exchange of access to data for services can be seen as reciprocal. What counts as reciprocal follows from the nature of the service. In general: the more someone is willing to invest in a service, in terms of time, efforts and access to data, the more they receive in terms of the service levels. Making such value models explicit may strongly contribute to reciprocity and transparency in B2C contracts in private law.

40. What also becomes clear from the discussion, is that these kinds of data driven services are co-created in a joint effort between service provider and service consumer.[97] The service provider offers services, which are built up from contributions of other users. The notion of service co-creation has recently received a lot of attention in marketing literature. Several authors have observed a shift in commercial transactions from a dominant goods logic, towards a dominant service logic.

Further research is needed, in particular about ownership of the resources being contributed by a community of users (data; contributions; content). In the discussion above, we noted that services are co-created. The service provider helps to create a pool of resources, from which new services can be offered. In the current data practices, the service provider acts as the de facto owner of the pool of resources. By signing a privacy policy, individuals often give up the exclusive right to control the data about them. However, we could also see the service provider as a mere custodian of the resources. Under such a model, only usufruct of the data is rented to the service provider, but ownership remains with the data subject. Smart contracts about data usage might contain a range of data rights as counter offer: access right, right to share, usufruct, lease for a period, or full ownership.

We believe that our idea to move part of the data protection discussion into contract law, and our detailed approach of negotiating, monitoring and enforcing smart contracts about data usage, can facilitate adoption of such other types of rights in a contract. Ultimately, such contracts would empower consumers to take back control over their data.

---

97 C. Grönroos & P. Voima, 41. *Journal of the Academy of Marketing Science* 2013, pp 133–150.