jipitec

1 | 2017

Volume 8 (2017)
Issue 1 ISSN 2190-3387

Special Issue on Contracts on Digital Goods and Services

Current Article

Practice Issues

Book Review

Journal of Intellectual Property, Information Technology, and Electronic Commerce Law

www.jipitec.eu

jipitec

Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Volume 8 Issue 1 April 2017
www.jipitec.eu
contact@jipitec.eu

A joint publication of:

Prof. Dr. Thomas Dreier, M. C. J.,
Karlsruhe Institute of Technology,
Vincenz-Prießnitz-Str. 3,
76131 Karlsruhe

Prof. Dr. Axel Metzger, LL. M.,
Humboldt-Universität zu
Berlin, Unter den Linden 6,
10099 Berlin

Prof. Dr. Gerald Spindler,
Dipl.-Ökonom, Georg-August-
Universität Göttingen,
Platz der Göttinger Sieben 6,
37073 Göttingen

Karlsruhe Institute of Technology, Humboldt-Universität zu Berlin and Georg-August-Universität Göttingen are corporations under public law, and represented by their respective presidents.

ISSN 2190-3387

Funded by

DGRI Deutsche Gesellschaft für Recht und Informatik e.V.

Table Of Contents

Special Issue on Contracts on Digital Goods and Services

Current Article

Practice Issues

Book Review

Editorial

Special Issue on Contracts on Digital Goods and Services

Recommended citation: Axel Metzger and Heike Schweitzer, Editorial: Special Issue on Contracts on Digital Goods and Services, 8 (2017) JIPITEC 1, para 1.

1 The European Commission's proposal for a Directive on contracts for the supply of digital content[1] has provoked a lively debate regarding the rights and duties of consumers of digital content, and about the rights and duties of service providers. The Commission's proposal addresses the legal characterization of contracts for the supply of digital content, their interoperability and portability, the consequences of conceiving data as counter-performance, the consumer's right to retrieve data and content, and a number of other relevant issues at the intersection of contract law, information technology, intellectual property and competition law. However, the proposed directive also contains remarkable gaps which are left to be filled by national laws of the member states. The political and academic debate on contracts for the supply of digital content is currently mainly focussed on the European legislative procedure. However, discussions on the member states' level with regard to the implementation of the Directive are already in sight.

2 Against this background, the authors of this editorial organized a conference on "Contracts on Digital Goods and Services" which was held at Humboldt-University, Berlin on October 6, 2016. The presentations given at the conference engendered intense discussions among the participants, who ranged from academics and legal practitioners to representatives from European and national governmental entities and stakeholders. This special issue features some of the papers presented at the conference. *Axel Metzger* (Berlin) carries out a contract law analysis of data as counter-performance and asks what rights and duties parties have. *Yoan Hermstrüwer* (Bonn) provides a behavioural economic analysis of big data and consent. *Hervé Jacquemin* (Namur) explores the characterization of contracts on the supply of digital content from a French and Belgian perspective. *Heike Schweitzer* (Berlin) and *Wolfgang Kerber* (Marburg) provide a legal and economic analysis of interoperability in the digital economy. *Ruth Janal* (Berlin) investigates data portability both under the General Data Protection Regulation and the proposed Directive on contracts for the supply of digital content. We would like to thank the editor-in-charge and his team for the possibility to publish the papers from the conference in a special issue of JIPITEC!

Axel Metzger
Heike Schweitzer

1 Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, COM/2015/0634 final - 2015/0287 (COD).

Data as Counter-Performance

What Rights and Duties do Parties Have?

by **Axel Metzger**, Dr. iur., LL.M. (Harvard), Professor of Law, Humboldt-Universität zu Berlin

Abstract: Article 3 para. 1 of the proposed Directive on certain aspects concerning contracts for the supply of digital content recognises that consumers may use their personal data as counter-performance in exchange for contents or services. This approach confirms a social practice, which may be observed everywhere in the digital environment. Accepting personal data as counter-performance in bilateral contracts intensifies the rights and duties of both parties. For the consumer, the proposed Directive clarifies that the data subject providing its personal data to the supplier shall have the same rights as in the case of a money consideration paid to the supplier. However, what are the duties of the consumer and what are the rights of the supplier? The proposed Directive does not address this issue. The article provides some initial answers based on German contract law.

Keywords: Digital content; contracts; consumer; personal data as counter performance; directive; contract law

Recommended citation: Axel Metzger, Data as Counter-Performance: What Rights and Duties do Parties Have?, 8 (2017) JIPITEC 2 para 1.

A. Introduction

1 The legal construction of "free services" on the Internet, which are provided to consumers while their personal data is requested or harvested, is currently undergoing a change of paradigm. Until recently, service providers like social media services, search engines, communication services, and hosting platforms, presented their business model as purely ad-funded services based on a two-sided market, in which the advertisers pay for the service and the users only have the advantages of attractive and cost-free services.[1] If the service asked the users consent to any data processing, this consent was treated under the old paradigm as being independent from the supply of the service. This idea of two independent legal transactions – supply of service and transmission of data – has been criticised by some commentators in recent years.[2] The European Commission's - Proposal for a Directive on certain aspects concerning contracts for the supply of digital content of December 2015[3] (DSDC) may now change the landscape.

B. Which scenarios are covered by the Directive?

2 The DSDC proposes to introduce harmonised rules on contracts for the supply of digital content in a broad sense, also comprising many services contracts, including services allowing the creation, processing, or storage of data and services allowing sharing of and any other interaction with data in digital form provided by other users of the service, see Art. 2 N° 1. For all those contracts, Art. 3 para.

1 See, e.g., <www.facebook.com>: "Sign Up. It's free and always will be."

2 See e.g. *Bräutigam* MMR 2012, 635; *Buchner* DuD 2012, 39, 41; *Rogosch*, Die Einwilligung im Datenschutzrecht, 41.

3 COM(2015) 634 final.

1 DSDC explicitly provides that the Directive shall apply to any contract where the supplier supplies digital content to the consumer "and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data." The language of Art. 3 para. 1 DSDC is broad and seems to cover all cases in which the service providers use the personal data of the consumer as the basis for the refunding of its service. However, the Commission's concept is more restrictive and covers only actively provided data. According to Recital 14, the Directive should apply only to contracts where the supplier requests and the consumer actively provides data, such as name and e-mail address or photos. To the contrary, the Directive should not apply to situations where the supplier collects data necessary for the digital content to function in conformity with the contract; for example geographical location for a mobile application to function properly. Additionally the Directive should not apply to situations where the supplier collects information, including personal data, such as the IP address, or other automatically generated information such as information collected and transmitted by a cookie, without the consumer actively supplying it. If the final text of the Directive would exclude all the scenarios mentioned in Recital 14, its scope of application would be rather limited. Yet, the Draft Report of the European Parliament's Committee on Legal Affairs sets forth a proposal to give the provision a broader scope and to include cases in which the personal data is "collected by the supplier or a third party in the interest of the supplier".[4] It is indeed hardly convincing to exclude personal data collected by the service provider – e.g. search terms, geographical location data etc. – if such data is processed and used beyond the usage necessary for the functioning of the service.[5] Such a processing of personal data will regularly depend on the consumer's consent.[6] Thus, the consumer provides a valuable counter-performance in exchange for the service and should profit from the protection given by the Directive. The same is true for data whereby the collection of which was initially strictly necessary for the performance of the contract or for meeting legal requirements, if the supplier later continues to process the data for commercial purposes, e.g. if a streaming service later uses data on the supplied content to offer other content or services to the consumer.

4 Draft Report of the Committee on the Internal Market and Consumer Protection and of the Committee on Legal Affairs 7.11.2016, C80394/2015 – 2015/0287(COD) drafted by MEPs *Evelyne Gebhardt* and *Axel Voss*.

5 See *European Law Institute*, Statement on the European Commission's Proposed Directive on the Supply of Digital Content to Consumers, 15-16; *Faust*, Digitale Wirtschaft – Analoges Recht, Gutachten zum 71. Deutschen Juristentag, 2016, A 18; *Spindler* MMR 2016, 147, 149-150.

6 But see *Härting* CR 2016, 735-740.

C. Contract Formation

3 The DSDC provides rules on the supply and conformity of digital content, on the rights and obligations of the parties, and on the termination of the contract. It does not harmonise the rules on the formation of contracts, especially in case of personal data as counter-performance, see Art. 3 para. 9. This leaves some of the most important practical legal issues raised by contracts with data as counter-performance to national law, as determined by Art. 3, 4 and 6 of Regulation 593/2008 on the law applicable to contractual obligations (Rome I).[7] The following analysis is based on the application of German law. Other jurisdictions will encounter comparable problems.

4 The first requirement for the formation of a contract with personal data as counter-performance is a respective offer to conclude such a contract. In terms of typical contracts for the supply of digital content, it will be the service provider who offers to conclude a contract for the use of its service.[8] It is therefore a question of interpretation of the terms and conditions of the service, of the explanations on the website, and the general appearance of the service, whether the service provider offers to conclude a contract with personal data as counter-performance. This interpretation, according to German contract law, is based on objective standards, as stated in section 157 of the German Civil Code: "Contracts are to be interpreted as required by good faith, taking customary practice into consideration." The decisive test is therefore how an average and reasonable addressee would understand the declarations and conduct of the service provider. In this regard, empirical evidence from Germany shows that users understand "free" services as services they pay for with their personal data. In a recent study[9] conducted in 2014 with 1002 randomly chosen German Internet users, 67% declared that they acknowledge that delivery of personal data and consent in data processing is a method of payment for Internet services. It is therefore quite plausible that an average user of a data-driven Internet service will understand an offer for a "cost-free use" in fact as an offer to exchange his or her personal data against the service.

7 The parties may choose the applicable law according to Art. 3 Rome I based on the service terms and conditions. However such a choice may not deprive the consumer from the protection afforded to him by the law of his habitual residence under the conditions of Art. 6 para. 1, 2 Rome I.

8 See e.g. the terms and conditions of <www.xing.com/terms>, <de-de.facebook.com/terms>, <www.amazon.de/gp/help/customer/display.html?ie=UTF8&nodeId=505048>.

9 See DIVSI, Daten – Ware und Währung, Hamburg 2014, <www.divsi.de/wp-content/uploads/2014/11/DIVSI-Studie-Daten-Ware-Waehrung.pdf>, 16.

5 Acceptance of such an offer may be declared explicitly, especially by ticking boxes, or implicitly by mere use of the service. German contract law has developed several means to avoid formalistic obstacles. According to section 151 sentence 1 German Civil Code, a contract comes into existence through the acceptance of the offer without the offeror needing to be notified of acceptance, if such a declaration is not to be expected according to customary practice. Based on this provision, it is well established in court practice that the use of Internet services may be interpreted as acceptance of the contract offer to use the service in accordance with the terms and conditions.[10] With regard to services that process the data of the users, one could even go further and understand such data processing as an indicator that the service has taken note of the user's acceptance of the contract terms.

D. Validity of the contract

6 As to the validity of contracts, several issues deserve attention. The validity of the contract for the supply of digital content will not be harmonised by the DSDC, but will remain in the realm of autonomous national contract law, Art. 3 para. 9 The validity issues are diverse and complex and can only be sketched out here.

I. Contracts with minors

7 The principles of contract law may conflict with the principles of data protection law, if a minor concludes a contract which comprises a counter-performance in the form of personal data. This scenario is apparently of high practical importance, given the relevancy of social media and other Internet services for juveniles. According to general contract law, at least in Germany, the validity of the contract depends on the authorisation given by the parents. The known exceptions to this principle, especially contracts which are legally beneficial for the minor according to section 107 German Civil Code or contracts performed with "pocket money" according to section 110 German Civil Code, do not match the case.[11]

8 Consent in data protection law follows different principles, see Art. 8 General Data Protection Regulation 2016/679 (GDPR): "The processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child." Member States may determine a lower age than 16 "provided that such lower age is not below 13 years". One way to solve this inconsistency is to separate the contract on the one hand and the delivery of data and consent of the minor on the other hand.[12] For the contract with all its consequences, the stricter general contract law principles of minor protection must be respected. If the parents have not authorised the contract, it must be regarded as void. Still, the consent given by the minor could be regarded as valid based on Art. 8 GDPR. The consequences of such a split solution would not be significant in most cases given the fact that consent is nevertheless revocable according to Art. 7 para. 3 GDPR. If the minor objects to any use of his personal data, they may revoke the consent for the future without further requirement. The only remaining question then would be whether the service provider must restitute the profits made before the revocation of the consent. Given the fact that Art. 7 and 8 are mainly focussed on unilateral declarations of consent, one could well argue that the stricter national principles for the conclusion of contracts with minors should also apply to the minor's consent if it has been given in the framework of a contractual relationship. As a consequence, contract and consent would be void.[13] The minor could then claim for damages for the unauthorised use of his data, which leads to the difficult follow-up question of how courts should assess the economic value of the data set of a single person.[14]

II. Privacy policies as standard terms and conditions

9 The consumer's consent in the processing of his data is typically based on the service provider's privacy policy. Such privacy policies are standard terms in the sense of Directive 93/13/EEC on unfair terms in consumer contracts and must therefore comply with the requirements of fairness and transparency. This

10 See e.g. LG Frankfurt am Main CR 2006, 729, 731.

11 See *Bräutigam* MMR 2012, 635, 637; *Jandt/Roßnagel* MMR 2011, 637, 639-640.

12 Compare *Faust*, Digitale Wirtschaft – Analoges Recht, Gutachten zum 71. Deutschen Juristentag, 2016, 8 et seq.

13 See *Metzger* AcP 2016, 817, 839-840 for German law.

14 Reliable economic data on the value of a set of personal data is not available yet. Facebook's price paid for WhatsApp is often cited as a proxy: 55 $ per user, see <www.bloomberg.com/news/articles/2014-10-28/facebook-s-22-billion-whatsapp-deal-buys-10-million-in-sales>. Other criteria may be taken from the pricing mechanism of services like <datacoup.com> who offer to pay money for the use of personal data. From the German legal academic literature see *Schwartmann/Hentsch* PING 2016, 117, 125, who value the data set of car from a three years lease contract at 1.500-2.000 €. See also *Wandtke* MMR 2017, 6.

is also emphasised by Recital 42 GDPR.[15]

10 Regarding the assessment of fairness, one may discuss whether the provision of data by the consumer and his/her consent are the "main subject matter" of the contract and as such exempted from the assessment of their fairness according to Art. 4 para. 2 of the Unfair Terms Directive. However, even if one applies Art. 4 para. 2, such an exemption should only cover the transfer of data and the consent as such, but not the specific conditions laid down in the privacy policies. German courts have repeatedly judged terms in privacy policies as being unfair in the sense of Art. 3 para. 1 of the Unfair Terms Directive if the purpose of the data processing was drafted in vague and unspecific language.[16] This jurisprudence is in line with both the Unfair Terms Directive and the GDPR.[17]

11 Regarding the transparency of privacy policies, Art. 7 para. 2 GDPR specifies the more general requirements from the Unfair Terms Directive. According to Art. 7 para. 2 GDPR, the service provider's request for consent "shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language." One may have doubts whether lengthy and detailed privacy policies, even if drafted in accordance with the cited requirements, can help to balance information asymmetries and to ensure that the consumer takes a rational decision with regard to his personal data.[18] Still, even if consumers do not read privacy policies they can still rely on the fact that privacy policies which are incompatible with the general principles of the GDPR do not meet the fairness test of the Unfair Terms Directive and may therefore not be enforced.[19]

III. Dependency of consent and service

12 A specific validity concern for contracts with personal data as counter-performance is raised by Art. 7 para. 4 GDPR: "When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract." At first glance, the rule seems to provide a clear ban of contracts that establish a link between the consent of the data subject and the provision of a service.[20] According to Article 3 para. 8, the DSDC is "without prejudice to the protection of individuals with regard to the processing of personal data." Thus, the DSDC cannot supersede the GDPR. Does this mean that, at the end, there is no such thing as data as counter-performance? Such a conclusion would certainly be premature. It would ignore that the European legislature of the DSDC apparently wanted to permit data as counter-performance. The solution must be found in a coherent interpretation of both texts. The wording of Art. 7 para. 4 GDPR is flexible: "Utmost account shall be taken" does not regulate a clear prohibition of data as counter-performance. Therefore, the provision may also be interpreted as an appeal to contracting parties and courts to pay special intention to the voluntary nature of the consumer's consent when consent is given within the framework of a contractual relationship. The question is whether consent has been given freely. Factors that may support the voluntary nature of the consumer's consent are the existence of competing services, the non-essential or dispensable character of the service for the consumer, and the character of the service as recreational or professional etc. It would be simplistic to infer from the mere wish of a consumer to use a service or to be part of a social network to a coercion effect.[21]

15 "In accordance with Council Directive 93/13/EEC a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms."

16 See e.g. KG CR 2014, 319 on the privacy policy of Facebook.

17 See Art. 6 para. 1 lit. a): "1. Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes (...)."

18 *Faure/Luth* Journal of Consumer Policy 34 (2011) 337–358.

19 See *Adams*, Ökonomische Analyse des Gesetzes zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen (AGB-Gesetz), in Neumann (ed.), Ansprüche, Eigentums- und Verfügungsrechte, 1983, 655, 664; *Basedow* in Münchener Kommentar zum BGB, 7th ed., 2016, Vorbemerkung zu § 305, N° 4-5; *Beimowski*, Zur ökonomischen Analyse Allgemeiner Geschäftsbedingungen, 1989, 15.

20 See also the very restrictive language in Recital 43 GDPR: "Consent is presumed not to be freely given (...) if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."

21 See also *Frenzel* in Paal/Pauly (ed.), Datenschutz-Grundverordnung, 2017, Art. 7, N° 18-21; *Plath*, BDSG/DSGVO, 2016, Art. 7, N° 14-16; *Schantz* NJW 2016, 1841, 1845. Compare also the more restrictive interpretation by *Albrecht* CR 2016, 88, 91.

E. Parties' obligations

I. Obligations of the supplier and the consumer

13 The DSDC is mainly focussed on the consumer's rights and the supplier's obligations and leaves the consumer's duties in the realm of autonomous national contract law.[22] According to Article 5 DSDC, the supplier shall supply the digital content to (a) the consumer or (b) a "third party which operates a physical or virtual facility making the digital content available to the consumer or allowing the consumer to access it and which has been chosen by the consumer for receiving the digital content".[23] Besides the fact that Art. 3 confirms the possibility to use data as counter-performance, the DSDC does not further specify the contractual obligations of the consumer in such a case.

14 This one-sided approach of the DSDC raises the question of whether one may construe a bilateral contractual relationship between the consumer and the service provider with personal data as counter-performance, which does not recognise any obligations of the consumers or contractual rights of the service provider. The answer must be found in light of two principle considerations. First, if one accepts data as an alternative "counter-performance", one may hardly deny the contracting party to claim for that counter-performance. Any other interpretation would neglect the fact that the service provider supplies the digital contents in exchange for the data and vice versa. Second, the binding effect of such a contract cannot undermine the right of the consumer to revoke his consent at any time. The duty of the consumer is therefore limited by the consumer's right to withdraw the consent at any moment. Nonetheless, this limitation does not change the correlation between the rights and duties of the supplier and the consumer. The supplier provides its service in exchange for the consumer's data even if his consent is revocable. "Synallagmatic contracts" with a right for one party to withdraw its consent are not unknown to the traditional contract law theory, at least in Germany.[24]

15 Another question concerns accuracy and updating of personal data. Terms and conditions of typical platforms oblige the user to submit correct data and changes to the data, examples are Xing ("The user is obliged (a) to provide only true and non-misleading statements along with its real name, and to refrain from using pseudonyms or pen names ...")[25], Facebook ("Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account...")[26] or Amazon ("You are responsible for ensuring that the details you provide us with are correct and complete, and for informing us of any changes to the information you have provided.")[27] If the consumer, who submits data as counter-performance, may claim to be treated on equal footing as a paying customer, why then should the service provider not have the right to claim for such personal data as they could claim for the payment of the money consideration? It is the very nature of a contract to be bound by the promises given. Still, a duty to update the personal data without a respective request of the service provider should be assessed as being unfair in the sense of Art. 3 para. 1 of the Unfair Terms Directive. The average consumer does not read terms and conditions or privacy policies. If an update clause was valid, consumers would be in breach of contract without being aware of it. Services should therefore ask their customers from time to time for an update.

II. Failure to supply

16 The consumer may immediately terminate the contract, if the service fails to supply, Art. 11, 13 DSDC.[28] In addition, the consumer may claim for damages in accordance with Art. 14 DSDC, which limits the damage claim to the "economic damage to the digital environment of the consumer", a restriction which has been thoroughly criticised.[29]

17 By contrast, if the consumer fails to supply his data although he promised to, the service provider can only rely on national law. Under German law, the service provider may terminate the contract in accordance with section 323 German Civil Code. Moreover, the service provider may claim for damages on the basis of section 281 German Civil Code. Both remedies require that the supplier has specified, without result, an additional period for performance or cure. To award damages under

22 Recital 10.

23 See Art. 5 DSDC.

24 See, e.g., *Westermann* in Erman (found.), Bürgerliches Gesetzbuch, 14th ed., 2014, Vor § 320, N° 5 et seq.

25 <www.xing.com/terms>.

26 <www.facebook.com/terms>.

27 <www.amazon.de/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=201909000>.

28 See the critical comment of the European Law Institute, Statement on the European Commission's Proposed Directive on the Supply of Digital Content to Consumers, 27-28 for cases in which a digital product is developed to the consumer's specification.

29 *European Law Institute*, Statement on the European Commission's Proposed Directive on the Supply of Digital Content to Consumers, 32; Spindler MMR 2016, 219, 222.

section 281 German Civil Code is only consequent given the fact that the supplier has fulfilled his own contractual obligations but has not received the promised counter-performance. Such a claim for damages again raises the question how courts should assess the value of a concrete data set of a consumer.[30]

III. Lack of conformity

18 Lack of conformity of the digital content, as defined by Art. 6 DSDC[31], leads to the remedies specified in Art. 12, 13 DSDC. The service provider must bring the digital content into conformity, otherwise the rules on termination and damages may be applied.

19 By contrast, if the submitted data is incomplete or incorrect, the national contract law principles on non-conformity apply. The German Civil Code provides different remedies for cases of non-conformity depending of the nature of the contract, especially for sale, service, and lease contracts. Contracts on the submission of personal data are not regulated in German contract law so far. One obvious solution would be to apply the principles that have been developed for license contracts. Courts and commentators agree that license contracts should be treated analogous to the provisions on lease contracts with regard to the issue of non-conformity.[32] The service provider could claim for the submission of correct data, section 535 German Civil Code, for a restitution of the value of its own performance (instead of a rent reduction, section 536), for damages, section 536a, and for the termination of the contract in accordance with section 543 German Civil Code.

F. Termination

20 The DSDC provides detailed rules for the right of the consumer to terminate the contract, whereas it remains silent on the termination right of the supplier.

21 Where the supplier has failed to supply the digital content in accordance with Art. 5, the consumer is entitled to immediately terminate the contract in accordance with Art. 11 and 13.[33] If the digital content has been supplied but is not in conformity with the contract, the consumer may terminate the contract under the conditions of Art. 12 para. 3. Long term contracts may be terminated any time after the expiration of the first 12 months, Art. 16 DSDC.

22 The effects of the termination of the contract in case of data as counter-performance are provided for in Art. 13 and 16 DSDC. Art. 13 para. 2 lit. b) provides that the supplier shall take all measures "which could be expected in order to refrain from the use of the counter-performance other than money which the consumer has provided in exchange for the digital content and any other data collected by the supplier in relation to the supply of the digital content including any content provided by the consumer (...)". Other duties of the supplier in case of termination concern the portability of data and user generated content retained by the supplier, Art. 13 para. 2 lit. c).[34] Art. 16 para. 4 provides similar rules for the termination of long-term contracts. What is not provided for in the DSDC is a claim for restitution of the profits made by the supplier based on the consumer's data before termination. However, given the full-harmonisation approach of the DSDC, it seems hardly conceivable to refer to national law for such a claim.

23 The right of the supplier to terminate the contract is left to national law. If German law is applicable, the supplier has a right to terminate the contract in accordance with sections 323, 535 et seq. German Civil Code if the consumer fails to supply the promised data, or in case of a lack of conformity of the data as discussed in section E of this article. Such a termination has an effect ex post. This means that the consumer may be obliged to compensate the supplier for the use of digital content before the termination of the contract, see section 346 para. 1 and 2 German Civil Code. In addition, the supplier must have a right to terminate the contract without notice in application of section 543 para. 2 N° 1 German Civil Code, if the consumer withdraws its consent in the use of the data.[35] Such a termination only has effects on the future. For the time period in which the supplier could legally use the consumer's data, the supplier may not claim for compensation of the use of the digital content.

30 Supra Fn. 14.

31 See the deviating concept of conformity in the Draft Report of the Committee on the Internal Market and Consumer Protection and of the Committee on Legal Affairs 7.11.2016, C80394/2015 – 2015/0287(COD) drafted by MEPs *Evelyne Gebhardt* and *Axel Voss*.

32 BGH GRUR 2006, 435; see also BGH CR 2007, 75 f.; Hoeren, IT-Vertragsrecht, 2nd ed., 2012, 251 ff.; *Marly*, Praxishandbuch Softwarerecht, 6th ed., 2014, N° 752 et seq.

33 But see supra Fn. 28.

34 The portability provision must be read in context with Art. 20 GDPR. See the contribution of *Janal* in this issue of JIPITEC; see also *Spindler* MMR 2016, 219, 221-222.

35 See also *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 272 et seq.; *Langhanke/Schmidt-Kessel* EuCML 2015, 218, 222; *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 137.

G. Conclusions

24 The acknowledgement of personal data as counter-performance by Art. 3 para. 1 is one of the innovative elements of the proposed Directive on certain aspects concerning contracts for the supply of digital content. Empirically it is nothing more than the approval of a social practice which may be observed everywhere in the digital environment. "Free services" are often services by which the supplier earns his money with the processing of the data of its customers. From this perspective, the idea of data as counter-performance seems rather trivial. Still, the legal recognition of a common social practice, as has been shown in this article, will lead to legal consequences for both parties to the contract. Accepting personal data as counter-performance in bilateral contracts intensifies the rights and duties of both parties. For the consumer, the proposed Directive makes clear that the data subject providing his personal data to the supplier shall have the same rights as in the case of a money consideration paid to the supplier. However, what are the duties of the consumer and what are the rights of the supplier? The proposed Directive does not address the issue. This article has argued, based on German contract law principles, that the service provider should have the right to claim for the counter-performance within the limits of data protection law. As a consequence, the consumer is under an obligation to submit his data in accordance with the terms and conditions (and the privacy policy) of the supplier. However, the consumer can revoke his consent at any moment in the future. This combination of European law for the rights of one party and national law for the rights of the other party raises a number of fundamental challenges, especially in light of the full harmonisation approach of the Directive and the principle of effectiveness of European law. Whether the Directive will finally improve the legal situation of consumers on the digital markets will also depend on the protection given to the supplier on the national level. On the one hand, it will hardly be acceptable to give full protection to the consumer "paying with its personal data" without looking at the same time at the suppliers rights in such contract settings. On the other hand, the rights of the supplier in application of the national contract law may also not undermine the legislative purpose of the Directive. The coming years will have to show exactly where the line should be drawn between these two interests. If at the end the consumer will face an intensified catalogue of obligations towards suppliers, the implementation of Art. 3 would still have a positive effect for consumers. Accepting personal data as counter-performance will at least strengthen transparency and raise awareness of the economic value of personal data and as such foster the rational behaviour of consumers.

Contracting Around Privacy

The (Behavioral) Law and Economics of Consent and Big Data

by **Yoan Hermstrüwer**, Senior Research Fellow at the Max Planck Institute for Research on Collective Goods in Bonn, Germany. His research covers (behavioral) law and economics, cyberlaw, constitutional law, financial law, international economic law and empirical legal studies (hermstruewer@coll.mpg.de).

Abstract: European privacy law rests on the implicit assumption that consent to the processing of personal data and the analysis of Big Data is a purely individual choice. Accordingly, privacy lawyers mainly focus on how to empower users to make free and informed choices, for instance through debiasing and nudging. However, a game theoretical analysis suggests that strategic considerations may be a driving force of consent under certain conditions. In environments relying on the use of Big Data, consent is likely to impose negative privacy externalities on other users and constrain their freedom of choice. By contrast, a behavioral economic analysis suggests that users are subject to bounded rationality and bounded willpower. While nudges, like default options, can enable users to make protective privacy choices in some cases, correcting cognitive deficits might facilitate market failures and accelerate the erosion of privacy in other cases. This counterintuitive conclusion shows that legal rules on consent and privacy contracts should be grounded on an assumption of 'mixed rationalities', i.e. on insights from both standard economics and behavioral economics. Hence, a sharper distinction between 'paternalistic nudging' and 'non-paternalistic soft regulation' to counter market failures is warranted.

Keywords: Consent; monetizing personal data; big data; EU privacy law; EU-GDPR; behavioral law and economics; game theory; nudging, libertarian paternalism; constitutional law

Recommended citation: Yoan Hermstrüwer, Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data, 8 (2017) JIPITEC 9 para 1.

A. Introduction

1 Personal data has become one of the most important currencies in digital economies.[1] This currency seems to be inherently inclusive and egalitarian, since there is no need to be wealthy in order to pay with data. Digital services like Facebook, Google, Instagram or Snapchat, largely rely on this *pay-with-data* business model and the use of Big Data. However, monetizing personal data might well give rise to a society where, overall, publicity trumps privacy. On both sides of the Atlantic, the debate about what legislators should do to cope with the tendency to contract around privacy and the continuous erosion of privacy has just begun.

2 One of the biggest problems is that privacy law does not really dovetail with the concept of contract and the idea of personal data as money.[2] While there is a growing consensus that privacy can be waived and even monetized, it is less clear under which conditions such a 'contract around privacy' shall be considered valid. In the draft of a Directive on

1 This article draws on Hermstrüwer, Informationelle Selbstgefährdung (2016).

2 *Ben-Shahar/Strahilevitz*, Contracting over Privacy: Introduction, Journal of Legal Studies 45 (2016), S1 (S5-S10); *Hermstrüwer*, Informationelle Selbstgefährdung (2016).

certain aspects concerning contracts for the supply of digital content, the European Commission has proposed a new legal regime for contracts "where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data".[3] The EU General Data Protection Regulation (EU-GDPR), which was recently adopted as a substitute for the EU Data Protection Directive, relies on consent as the prime mechanism to 'pay' with personal data.[4] According to Art. 4 § 11 EU-GDPR, consent "means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". How can privacy law enable people to make such an autonomous choice?

3 The academic and political struggle over appropriate tools to empower people to protect or waive their privacy has been fought from two different angles: the traditional data protection approach and the market-oriented approach. The data protection approach is firmly anchored in the tradition of public law doctrine and claims that stricter government interventions to protect privacy are needed.[5] The market-oriented approach basically claims that the market will yield an optimal level of privacy, be it through competition, self-regulation, or learning and evolutionary forces.[6]

4 In this article, I argue that to a certain extent both approaches go astray. As it seems, neither policymakers nor legislators have sufficiently taken account of the cognitive and motivational forces driving privacy choices. The result of this reluctance to take account of economics and psychology is a mismatch between the regulatory problem and the legal tools introduced to solve it. Consequently, the literature regarding the role that the behavioral sciences could play in the design and implementation of EU privacy law remains rather scarce.[7] To understand the regulatory problem associated with contracts involving consent to the disclosure of personal information, I argue that it is crucial to understand the behavioral and social forces that push people to disclose personal information in the first place. A cautionary note is warranted, however; the objective of my analysis is not to identify the criteria for optimal contract design, nor to develop a full-fledged doctrinal framework for consent and Big Data embedded in behavioral law and economics. Rather, my objective is to identify some of the 'sweet spots' where the law could step in to regulate privacy choices and consent, given certain more or less specific objectives that EU privacy law aims to accomplish.

5 In Section B, I explore the factors driving consent in an analytical framework set out by rational choice theory and game theory. This approach allows us to understand some of the strategic reasons pushing users to disclose or withhold personal information in interactions with companies or other users. In Section C, I shed light on the so-called privacy paradox and the behavioral economics of privacy. Without a good grasp of this paradox, lawmakers and legal practitioners are likely to make ill-informed choices that may well cause backfire effects in some cases. In Section D, I show that a behaviorally informed privacy law does not necessarily imply libertarian paternalism. EU privacy law and constitutional law should take account of the distinction between paternalistic nudging and non-paternalistic soft regulation of market failures. In Section E, I present my conclusion.

B. The Strategic Rationality of Consent

6 Rational choice theory assumes that individuals are rational actors with a set of stable and exogenously given preferences.[8] Rational actors are able to process an indefinite amount of information and will always make their choices such as to maximize their utility. Standard game theory builds on the rational choice paradigm and analyzes strategic interactions between actors.[9] Under a game theory approach,

3 Art. 3 § 1 of the Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content [Brussels, 9.12.2015, COM(2015) 634 final].

4 Regulation EU 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

5 *Solove*, Privacy Self-Management and the Consent Dilemma, Harvard Law Review 126 (2013), 1880; *Weichert*, Wider das Verbot mit Erlaubnisvorbehalt im Datenschutz?, Datenschutz und Datensicherheit 2013, 246.

6 *Tene/Polonetsky*, Big Data for All: Privacy and User Control in the Age of Analytics, 11 Northwestern Journal of Technology and Intellectual Property 11 (2013), 239 (242), favoring a relaxation of the consent requirement; for a traditional view *Posner*, The Right of Privacy, Georgia Law Review 12 (1978), 393; *Stigler*, An introduction to privacy in economics and politics, Journal of Legal Studies 9 (1980), 623; *Posner*, The Economics of Privacy, American Economic Review 71 (1981), 405.

7 But see *Borgesius*, Behavioural Sciences and the Regulation of Privacy on the Internet, in Alemanno/Sibony (Eds.), Nudge and the Law: A European Perspective (2015), 179.

8 *Becker*, The Economic Approach to Human Behavior (1976), 14.

9 *Rebonato*, Taking Liberties: A Critical Examination of Libertarian Paternalism (2012).

whether a person gives their[10] consent depends on the choices or, more precisely, the strategies chosen by companies and other users. Consent has the features of a choice in a strategic game. Game theory shows that under certain conditions, rational actors will have a strategic incentive to disclose personal information and give their consent. The upshot is that the erosion of privacy does not necessarily result from the bounded rationality of users. Rather, consenting to the processing of personal information might often be the result of a rational calculus. On a *positive* view, this shows that countering bounded rationality could facilitate strategic choices for sophisticated users and accelerate the erosion of privacy. On a *normative* view, it shows the limits and potential drawbacks of debiasing instruments in the field of privacy law.

I. Consent and Default Rules

7 According to the Coase theorem, the initial allocation of a right or good is irrelevant for its final allocation in the absence of transaction costs.[11] The right or good will eventually end up in the hands of the person who values it most. Each transaction entails a pareto-superior allocation. The process ends once a pareto-optimal allocation is accomplished; and in principle, the same holds for the process of bargaining over the allocation of personal information. The main contribution of the Coase theorem is not that markets will work in theory, but that transaction costs matter. When transaction costs are high – as is usually the case – parties will not contract around inefficient default rules (contractual standard settings).[12] Therefore, the law should use instruments to reduce transaction costs when the legislator aims to foster efficiency (welfare approach) or to increase transaction costs when the legislator aims to limit transactions for whatever reason. What does this mean for situations where users and companies can bargain over the allocation of personal information?

8 On the one hand, privacy law can attempt to minimize the transaction costs associated with the transfer of personal information. This objective can be achieved through default rules. As regards consent and contract formation, privacy law distinguishes between two different types of default rules: opt-in rules and opt-out rules. Traditionally, law and economics scholars claim that default rules should mimic the terms that a majority of parties would have agreed on without transaction costs (*majoritarian defaults*).[13] A majoritarian default simply minimizes the number of parties that have to contract around a default rule to reach an efficient agreement. The theory of majoritarian defaults results from a simple transaction cost analysis of incomplete contracts.

9 The problem of this approach is that it assumes a symmetric distribution of transaction costs between the majority and the minority.[14] When it comes to the design of consent options in privacy law, such an asymmetric distribution of costs is not unlikely. Digital platforms can lower their transaction costs by offering a standardized menu of default rules in their privacy settings. Their transaction costs should be low because they do not have to bargain over privacy with each and every user. On the user side, however, one should expect a huge disparity of transaction costs. Suppose that most users do not care for privacy, while a minority of users has strong privacy preferences. If the number of default rules in the standardized privacy settings is large, like on Facebook or Google, the minority of privacy sensitive users will incur high transaction costs since they will have to alter most of the standardized privacy settings. The inverse problem arises when the majority of users have strong privacy preferences.[15] In this case, the small group of users with weak privacy preferences is likely to incur high transaction costs if the default rules restrict the processing of personal information. Without concrete empirical evidence on the distribution of transaction costs, legislators can only speculate about the adequate allocation of rights. This shows that the *privacy by default* principle enshrined in Art. 25 § 2 EU-GDPR cannot clearly be justified according to the logic of majoritarian defaults.

10 On the other hand, default rules may also be justified on strategic grounds to counter the risk of a specific kind of market failure. In some cases, the bargaining parties will refrain from contracting around a default rule even when the transaction costs are low. Parties might prefer to stick with the status quo because contracting around the default rule would require one of the parties to disclose private information.[16] Disclosure of this information might enable the

10 For the sake of linguistic neutrality, I avoid the generic 'he' or 'she' and use the *singular they* as far as possible. See *Baron*, Gender politics of the generic "he", OUPblog, January 6, 2016, *available at* <https://blog.oup.com/2016/01/gender-politics-generic-he/>.

11 *Coase*, The Problem of Social Cost, Journal of Law and Economics 3 (1960), 1.

12 *Korobkin*, The Status Quo Bias and Contract Default Rules, Cornell Law Review 83 (1998), 608 (614-615).

13 See *Ayres/Gertner*, Majoritarian vs. Minoritarian Defaults, Stanford Law Review 51 (1999), 1591 (1592).

14 *Ayres/Gertner*, Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules, Yale Law Journal 99 (1989), 87 (93).

15 *Willis*, Why Not Privacy by Default?, Berkeley Technology Law Journal 29 (2014), 61 (64).

16 *Korobkin*, The Status Quo Bias and Contract Default Rules, Cornell Law Review 83 (1998), 608 (617-618).

uninformed party to exploit this information to their benefit and increase their gains from the contract.[17] Building on this analysis, default rules can be set in a way that the parties – specifically the informed party – would not want (*penalty defaults*).[18] Penalty defaults follow the logic of signaling games in that they force the informed party to reveal information regarding their own attributes (type).[19] They are designed to give the informed party an incentive to disclose private information. Accordingly, an opt-in rule that requires consent sets an incentive for companies to reveal more or more specific information about the characteristics of the service and the respective privacy policies.[20] An opt-in rule will force companies to convince users to opt in and give their consent. Through the lens of the theory of penalty defaults, an opt-in rule may be justified as a rule to solve information asymmetries and counter market failures. On this view, it should not be conceived of as a policy default that aims at exploiting users' status quo bias and reducing the overall amount of positive consent decisions. Hence, the theory of penalty defaults might provide a better normative rationalization of Art. 25 § 2 EU-GDPR than justifications on the grounds of libertarian paternalism.

II. Consent and Collective Privacy

11 In a libertarian society, users have the right to disclose as much personal information as they like. The problem of this individualistic conception of privacy is that it misses a crucial feature of modern data analytics (Big Data) and the behavioral forces underlying the diffusion of personal information in networked environments. To understand the problem, it is helpful to consider a social network like Facebook or any other service building on network externalities. In these networks, algorithms are used to analyze large datasets consisting of personal and anonymized data.[21] For these algorithms to allow good predictions about personal traits and behaviors, the network operator needs two things: sound knowledge about the social graph and large amounts of data. The social graph describes the social ties between users.

12 Now suppose that Angela is best friends with Bartleby and that Angela has willingly revealed information about her sexual orientation, while Bartleby has refrained from doing so, since he 'would prefer not to'.[22] Empirical evidence suggests that it is possible to predict the probability of Bartleby's sexual orientation with a simple logistic regression that depends on one parameter, i.e. the number of friends with a known sexual orientation.[23] This kind of prediction is not deterministic but probabilistic. However, if the data set is large enough, regressions will usually generate a better prediction than the toss of an even-sided coin. Other traits such as ethnicity, political preferences, religious affiliation, addictive behaviors and even emotions can be inferred from seemingly unrelated data using psychometric methods.[24] The more information a user feeds into the algorithms, the easier it becomes to predict outcomes. Moreover, with every piece of information that people willingly reveal about themselves, they increase the probability of revealing personal information about other users regardless of their (the other users') consent. Technically speaking, consenting to the processing of personal information about oneself imposes negative privacy externalities on other users.[25] This shows that privacy in networked environments has the features of a social dilemma.[26]

13 The easiest way to conceptualize the problem that users face when confronted with the option to disclose personal information or withhold it, is a simple prisoners' dilemma (Figure 1).[27] Suppose that users have the opportunity to give their consent (Defect = D) or refuse their consent (Cooperate = C). Further, suppose that each user has an incentive to disclose certain types of information about herself – say because she obtains a monetary or social reward

17 *Ayres/Gertner*, Majoritarian vs. Minoritarian Defaults, Stanford Law Review 51 (1999), 1591 (1591).

18 *Ayres/Gertner*, Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules, Yale Law Journal 99 (1989), 87 (91).

19 The idea of signaling games is often attributed to *Spence*, Job Market Signaling, Quarterly Journal of Economics 87 (1973), 355.

20 *Kesan/Shah*, Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics, Notre Dame Law Review 82 (2006), 583 (633); *Willis*, Why Not Privacy by Default?, Berkeley Technology Law Journal 29 (2014), 61 (82).

21 *Mayer-Schönberger*, Big Data: A Revolution That Will Transform How We Live, Work, and Think (2013); *Fairfield/Engel*, Privacy as a Public Good, Duke Law Journal 65 (2015), 385 (389-390).

22 This is an allusion to *Herman Melville*, Bartleby, the Scrivener: A Story of Wall Street [The Piazza Tales, 1856].

23 *Jernigan/Mistree*, Gaydar: Facebook friendships expose sexual orientation, First Monday 14 (2009).

24 *Kosinski/Stillwell/Graepel*, Private traits and attributes are predictable from digital records of human behavior, PNAS 110 (2013), 5802 (5803). The rumor goes that Cambridge Analytica helped Donald Trump to win the US presidential election in 2016 by targeting thousands of users through psychometrics.

25 *MacCarthy*, New Directions in Privacy: Disclosure, Unfairness and Externalities, I/S: A Journal of Law and Policy for the Information Society 6 (2011), 425 (447).

26 See also *Regan*, Legislating Privacy: Technology, Social Values, and Public Policy (1995), 227; *Fairfield/Engel*, Privacy as a Public Good, Duke Law Journal 65 (2015), 385 (397).

27 For a more complex model see *Hermstrüwer*, Informationelle Selbstgefährdung (2016), 167-169.

– but that she does not want others to intrude on her privacy and disclose information about her.

		User 2 C	User 2 D
User 1	C	3 , 3	0 , 5
	D	5 , 0	1 , 1

Figure 1: Prisoners' dilemma

14 From a rational choice perspective, it is rational for every user to give their consent if the benefits of consent exceed its costs. In the prisoners' dilemma depicted above, consent is the best response to any given strategy of the other user.[28] In this simple game, consent (D) strictly dominates the refusal of consent (C), which means that each user will disclose personal information. Consent is the dominant strategy equilibrium in this game.

15 To understand the role of companies and the broader dimension of the social conflict over privacy, the interaction between users and companies may be conceived of as a one-sided hawk/dove game (Figure 2).[29] Suppose that companies can choose between an aggressive strategy of gathering data (Hawk = H) or a tame strategy of offering users a decent level of privacy protection (Dove = D). Further suppose that users can choose between consent (D) and the refusal of consent (H) and that companies have understood the social dilemma between users described above.

		Companies D	Companies H
Users	D	2 , 1	1 , 4
	H	4 , 0	0 , 2

Figure 2: One-sided hawk/dove game

16 If companies anticipate that only few users will refuse to give their consent or refrain from using their services, they will always opt for the aggressive strategy and impose take-it-or-leave-it options on users. From this point of view, refusing consent and the disclosure of personal information is not a credible threat against companies. Companies will anticipate that the group of users refusing consent will not be large enough to negatively affect their gains. Users can refuse consent but this choice excludes them from the use of digital services if no privacy-friendly alternatives are offered on the market. The important aspect of this game is that it combines elements of a cooperation game and a coordination game. As a consequence, the choice over the disclosure or non-disclosure of personal information may be described as a decision in a mixed-motive game in which users have to cooperate and coordinate to reach a socially optimal level of privacy. What does this analysis tell us about privacy law?

17 First, it shows that the individualistic conceptualization of privacy goes astray. The decision to give consent and disclose personal information will often be influenced by other users' behavior and result from strategic incentives in a situation with the features of a social dilemma. The refusal of consent is a dominated strategy that rational users will have no incentive to choose whatsoever. On this view, full and informed consent might be considered the reason for the erosion of privacy and not the solution to the very problem. The counterintuitive result for lawmakers and privacy lawyers is that empowering users to make more rational choices is likely to accelerate the erosion of privacy. This result holds regardless of individual privacy valuations.

18 Second, in larger networked environments the social dilemma will have the features of a public goods game. Users might have an incentive to free-ride on other users' efforts to protect their privacy and persist on disclosing personal information about themselves. In the end, consent is rational from an individual perspective but it produces a suboptimal level of privacy for all users. The individual freedom of users to give their consent comes at a cost, namely a reduction of the level of collective privacy. This leads to a crucial insight for legislators and privacy lawyers: Privacy law can either guarantee the freedom of consent or a (pareto-)optimal level of privacy, but not both.

19 This analysis prompts three conclusions regarding privacy regulation. First, experimental evidence on public goods games suggests that many people are conditional cooperators.[30] If people believe that

28 *Rasmusen*, Games and Information. An Introduction to Game Theory, 4. Ed. (2007), 20; *Baird/Gertner/Picker*, Game Theory and the Law (1994), 11-14.

29 For this conceptualization of the problem *Warner/Sloan*, Behavioral Advertising: From One-Sided Chicken to Informational Norms, Vanderbilt Journal of Entertainment and Technology Law 15 (2012), 49 (61-65). *Hetcher*, Norms in a Wired World (2004), 298-301, assumes a prisoners' dilemma and the evolution towards cooperative norms between companies and users in the long run.

30 *Fischbacher/Gächter/Fehr*, Are people conditionally cooperative? Evidence from a public goods experiment, Economics Letters 71 (2001), 397; *Chaudhuri*, Sustaining Cooperation in Laboratory Public Goods Experiments: A Selective Survey of the Literature, Experimental Economics

others will not exploit them or free-ride on their efforts, they are likely to resist the temptation of playing an uncooperative strategy. Increasing the visibility of other users' refusal to consent might be used as a tool to trigger reciprocation and cooperation among users. Second, theories of expressive law suggest that law can be used to communicate normative expectations and thereby change behavior without the threat of a sanction.[31] Expressive law can either induce a change of preferences or push people to select certain equilibria in strategic interactions. In the latter case, the law can be used to set what game theorists call a focal point. In principle, communication of the rule sets a focal point and helps solve the coordination problem.[32] For instance, increasing the salience of legal rules on right-hand or left-hand traffic is likely to make the preferred outcome focal. Empirical evidence suggests that focal points can facilitate equilibrium selection not only in pure coordination games but also in mixed-motive games.[33] Therefore, making opt-in rules very salient could set a focal point and help users solve some of the strategic problems associated with consent. Opt-in rules can be considered as third-party expression of normative (legislative) expectations as to the socially desirable level of privacy. They might help users to form an expectation of the behavior of other users. Third, empowering users to make informed and unrestricted choices about the disclosure of personal information is likely to accelerate the erosion of privacy in networked environments instead of slowing it down. The legal requirements set by Art. 7 § 1 EU-GDPR (free and informed consent) are based on a purely individualistic conception of privacy.

20 In sum, the EU-GDPR takes no account of collective privacy and the strategic incentive problems resulting from the analysis of Big Data. To solve the privacy problem, legislators and privacy lawyers might consider structural similarities with other public goods problems, such as the protection of the environment or the stability of the financial system.

III. Consent and Unraveling

21 Privacy lawyers often assume that refusing consent will offer sound protection of individual privacy.[34] Each user, the argument goes, can freely decide whether to disclose or withhold personal information. I have already explained why this argument is flawed once we consider the strategic incentives of users in environments with the features of a social dilemma and a one-sided hawk/dove game. But another problem might occur when consent is incentivized, the company creating the incentive holds a monopoly, and the group of users is heterogeneous.

22 For example, consider an insurance company that offers a rebate if the user consents to the disclosure of a specific piece of 'high-value' personal information – such as information about good health – and discriminates between different types of users.[35] In a pool of heterogeneous users, the user with the best health information has the strongest incentive to reveal this information and consent to its processing because they would like to obtain a favorable (cheaper) service. Once this user has consented, the pool of remaining users shrinks. The user who had the second-best personal traits now has the best personal traits in the pool of remaining users and therefore has the strongest incentive to give consent. This user would want to avoid a negative inference about their health status from a refusal of consent and therefore disclose personal information. An unraveling process has now been set in motion. This process follows the logic of signaling games where the disclosure of high-value information facilitates an inference about low-value information for those refusing to disclose personal information.[36] Without further constraints and with a tool to verify personal information, the unraveling process ends when every user has consented to the disclosure and processing of personal information.[37]

23 This unraveling may concur with price discrimination where the company aligns the price of the service with the individual willingness to

14 (2011), 47 (49).

31 *Lessig*, The New Chicago School, Journal of Legal Studies 27 (1998), 661; *McAdams*, A Focal Point Theory of Expressive Law, Virginia Law Review 86 (2000), 1649.

32 For an investigation of salience see *Mehta/Starmer/Sugden*, The Nature of Salience: An Experimental Investigation of Pure Coordination Games, American Economic Review 84 (1994), 658.

33 *McAdams/Nadler*, Testing the Focal Point Theory of Legal Compliance: The Effect of Third-Party Expression in an Experimental Hawk/Dove Game, Journal of Empirical Legal Studies 2 (2005), 87.

34 *Mayer-Schönberger*, Delete: The Virtue of Forgetting in the Digital Age (2009), 128-134.

35 The basic idea goes back to *Grossman*, The Informational Role of Warranties and Private Disclosure About Product Quality, Journal of Law and Economics 24 (1981), 461. See also *Fishman/Hagerty*, Mandatory Versus Voluntary Disclosure in Markets with Informed and Uninformed Customers, Journal of Law, Economics, and Organization 19 (2003), 45. For many more examples see *Peppet*, Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future, Northwestern University Law Review 105 (2011), 1153.

36 *Stigler*, An Introduction to Privacy in Economics and Politics, Journal of Legal Studies 9 (1980), 623.

37 *Baird/Gertner/Picker*, Game Theory and the Law (1994), 90.

pay.[38] However, both processes do not necessarily coincide. It is important to note that unraveling is efficiency-enhancing since users will be required to pay a price that reflects their individual (health) risk. Privacy has the opposite effect and entails a redistribution of resources between users and cross-subsidization of types with low-value information. Efficiency-minded users might therefore prefer a certain degree of unraveling, while users with a preference for redistribution might have a taste for privacy. However, whether an unraveling occurs in real markets will depend on a variety of additional factors.

24 First, if the company sets a certain quality threshold and only offers a rebate for personal information above this threshold – e.g. for doing sports three times a week – only users with information above this threshold will give their consent. This might eventually lead to a separating equilibrium with a pool of consenting users and a pool of non-consenting users.[39] In this case, unraveling is mitigated. Second, if the costs of consent are high, only few users will give their consent. Non-consenting users will be pooled together and include users with high-value and low-value information. It will then be difficult to make a sound inference from a refusal of consent. High costs of consent may therefore lead to a pooling equilibrium and limit unraveling.[40] Third, bounded rationality in the sense of limited depth of reasoning (level-k reasoning) and limited anticipation of other users' behavior may also slow down the unraveling process.[41] Only entirely rational players who form correct beliefs about other players' beliefs (about their own beliefs and so on) will eventually set in motion a perfect unraveling process. Finally, a simple privacy framing (e.g. mentioning that the choice relates to the 'health status' of 'workers' in a 'labor market') may be enough to trigger privacy concerns and reduce the propensity to consent.[42] Salient information about the risks of consent and the processing of personal information could therefore mitigate unraveling.[43]

25 Generally, this analysis shows that privacy law has rent-shifting effects.[44] User welfare depends on the distribution of user types and on the identity and distributional preferences of those who benefit or lose from privacy-protective rules. From a doctrinal point of view, it shows that conventional legal doctrines concerning the freedom of consent do not capture the behavioral pressure associated with unraveling. The implicit behavioral assumption of many privacy laws is that the freedom to consent is not constrained as long as users are formally offered an option to refuse consent and use the service without disclosing personal information. Under Art. 7 § 4 EU-GDPR, for instance, the assessment whether consent is freely given should take account of whether the performance of a contract is conditional on consent. However, as the unraveling analysis shows, consent may significantly increase the pressure to consent on other users. Once unraveling is triggered, consent imposes a negative externality on others in that it increases their (expected) cost of refusing consent. Unraveling might therefore occur irrespective of a conditionality link between contract performance and consent. This prompts two observations as to the adequacy of legal instruments used to protect privacy.

26 On the one hand, there are many situations where the most effective instrument to mitigate unraveling will be a legal prohibition of the processing of personal information. Art. 9 § 1 EU-GDPR contains such a prohibition for genetic data, biometric data, health data and data concerning sex life and sexual orientation. This prohibition is based on the conventional idea that specific categories of personal information should benefit from stronger protection than others. It does not however, take account of the structural risk of unraveling. If privacy law aims at securing the freedom of consent, it might make more sense to identify situations bearing a high unraveling risk and determine the level of privacy protection according to this risk instead of relying on a classification of specific categories of personal information deemed to be sensitive.

27 It is important to note that the legal justification for this kind of prohibition is not paternalistic. Rather, prohibitions of processing will have the effect of countering negative externalities (i.e. behavioral pressures generated by consent) and

38 For an analysis see *Strandburg*, Free Fall: The Online Market's Consumer Preference Disconnect, University of Chicago Legal Forum (2013), 95 (134-141).

39 For further explanations of this equilibrium concept see *Rasmusen*, Games and Information. An Introduction to Game Theory, 4. Ed. (2007), 320-324; *Baird/Gertner/Picker*, Game Theory and the Law (1994), 80-89.

40 *Posner*, Privacy, in: Newman (Ed.), The New Palgrave Dictionary of Economics and the Law 3 (1998), 103; *Benndorf/Kübler/Normann*, Privacy concerns, voluntary disclosure of information, and unraveling: An experiment, European Economic Review 75 (2015), 43 (48-52).

41 *Benndorf/Kübler/Normann*, Privacy concerns, voluntary disclosure of information, and unraveling: An experiment, European Economic Review 75 (2015), 43 (51-52). Inequality aversion could also reduce unraveling.

42 *Benndorf/Kübler/Normann*, Privacy concerns, voluntary disclosure of information, and unraveling: An experiment, European Economic Review 75 (2015), 43 (50).

43 However, salient consent options may push users to comply with social norms, see *Hermstrüwer/Dickert*, Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten, MPI Collective Goods Preprint, No. 2013/15 (<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2311201>).

44 *Jentzsch*, Secondary use of personal data: a welfare analysis, European Journal of Law and Economics (2014), 1 (21).

could be justified on non-paternalistic grounds. An unraveling-based legal rule should also consider whether users can influence personal information. Unraveling might have antisocial effects when personal information is impossible or costly to influence. In this case, privacy law might be used as a social policy tool to increase redistribution and reduce unraveling pressures on those who should benefit from redistribution. Finally, prohibitions could be based on the objective to reduce chilling effects.[45] Such chilling effects might occur where users are offered valuable rewards for high-value information and where they have an incentive to adapt their behavior to generate such information, e.g. do more sports when consent to the processing of information regarding intense sports activities is incentivized. The normative assessment of a chilling effect depends on whether a deviation from the expectation set by the data-intensive service is qualified as 'good'. Courts could operate this assessment on a case-by-case basis and use the unraveling argument as a justification for sectoral restrictions.

28 On the other hand, the unraveling argument shows that a correction of rationality deficits (*debiasing*) will not necessarily lead to an increase of privacy.[46] Improving users' capacity to engage in level-k reasoning and anticipate other users' behavior would probably foster unraveling. Providing users with better information about the inner-workings of algorithms and data-intensive services might not always be compatible with the objective of increasing the level of privacy. This prompts an argument that runs counter to the regulatory approach supported by some libertarian paternalists: If the social value to be protected is privacy according to the policy objectives formulated by the European legislator, reducing bounded rationality is likely to be the wrong intervention. The potential downside of such an approach is that some unsophisticated users would have to cope with the bounds of their rationality on their own.

C. The Behavioral Rationality of Consent

29 Instead of building an axioms known from decision theory, behavioral economists draw into question these very assumptions (money maximization[47], stability and exogeneity of preferences, optimal evaluation and processing of information).[48] Analyzing the trade-offs associated with protecting or sharing personal information, behavioral economists have determined bounds to rationality, self-interest and willpower.[49] These bounds provide some explanations of the factors pushing users to disclose personal information and give their consent. The starting point of the analysis is what has been called the privacy paradox: While many people claim that they do care very much about their privacy, they willingly reveal large amounts of personal information. This observation is corroborated by empirical evidence showing that there is a significant gap between expressed preferences and revealed preferences for privacy.[50] According to the theory of revealed preferences, observed privacy choices can be seen as a straightforward expression of true privacy preferences. Accordingly, the privacy paradox is seen as an artifact of a comparison of two very different things: attitudes and behavior.

30 This approach, however, neglects psychological evidence on preference uncertainty, i.e. the fact that some people hold weak preferences or do not fully understand their preferences.[51] Furthermore, behavioral economics casts doubt on the relationship between choice, self-interest, utility and welfare.[52] Empirical evidence suggests that people are reluctant to offset the monetary benefits of consent with the

45 For a discussion of chilling effects in the context of privacy *Richards*, The Dangers of Surveillance, Harvard Law Review 126 (2013), 1934 (1949-1952).

46 For a general discussion of debiasing *Jolls/Sunstein*, Debiasing through Law, Journal of Legal Studies 35 (2006), 199.

47 It is important to note that utility maximization is not excluded under the assumption of non-standard preferences, see *Bernheim/Rangel*, Behavioral Public Economics: Welfare and Policy Analysis with Non-Standard Decision-Makers, in Diamond/Vartiainen (Eds.), Behavioral Economics and Its Applications (2007), 7.

48 *Jolls/Sunstein/Thaler*, A Behavioral Approach to Law and Economics, Stanford Law Review 50 (1998), 1471 (1476); for a critical assessment *Posner*, Rational Choice, Behavioral Economics, and the Law, Stanford Law Review 50 (1997), 1551.

49 *Acquisti/Brandimarte/Loewenstein*, Privacy and human behavior in the age of information, Science 347 (2015), 509; *Acquisti/Taylor/Wagman*, The Economics of Privacy, Journal of Economic Literature 54 (2016), 442; *Acquisti*, Nudging Privacy: The Behavioral Economics of Personal Information, IEEE Security & Privacy, November/December 2009, 82; *Acquisti/Grossklags*, Privacy and Rationality in Individual Decision Making, IEEE Security & Privacy, January/February 2005, 26.

50 *Berendt/Günther/Spiekermann*, Privacy in E-Commerce: Stated Preferences vs. Actual Behavior, Communications of the ACM 48 (2005), 1; *Norberg/Horne/Horne*, The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, Journal of Consumer Affairs 41 (2007), 100.

51 *Lichtenstein/Slovic*, The Construction of Preference: An Overview, in Lichtenstein/Slovic (Eds.), The Construction of Preference (2006), 1.

52 For an analysis of this problem generally *Sen*, Rationality and Freedom, 2002, 27; *Kőszegi/Rabin*, Mistakes in Choice-Based Welfare Analysis, American Economic Review 97 (2007), 477; *Bernheim/Rangel*, Beyond Revealed Preference: Choice-Theoretic Foundations for Behavioral Welfare Economics, Quarterly Journal of Economics 124 (2009), 51.

costs incurred by a loss of privacy.[53] As it seems, most people carry the costs and benefits of consent in different mental accounts (mental accounting). While there is a general reluctance to pay for privacy, this does not mean that users are never willing to incur costs for data protection.[54] Rather, it suggests that privacy preferences or, more generally, privacy behaviors are context-dependent and determined by the psychological processes underlying choices.[55] The obvious challenge for privacy law results from the fact that it cannot capture and regulate every context feature that might push users to disclose personal information. One possible solution to this challenge is to determine some of the structural features that are to a large extent context-independent. From a regulatory and legal perspective, it is critical to understand the reasons that might explain the structural factors driving the privacy paradox. Without such an understanding, privacy law is likely to use the wrong instruments to empower people to make free and informed privacy choices. The features determined in the following sections are derived from empirical studies of privacy choices. While these studies should be taken with due caution, they still provide important insights about the behavioral factors that privacy law should take account of.

I. Impact of Information

31 Perhaps the most obvious explanation for the privacy paradox can be found in information asymmetries between users and companies. Empirical evidence suggests that many users simply do not know when, how, and to what extent personal information is gathered by companies. Further evidence shows that only up to 1 % of users actually open the End User Licensing Agreement to have a glance at it when downloading software.[56] In a natural experiment conducted by GameStation, for instance, a large fraction of users agreed to sell their immortal soul when placing an order online.[57] This kind of behavior is not necessarily due to bounded rationality – regardless of whether users believe in the immortality of their soul or not. On the contrary, it is rational to refrain from reading privacy policies if the costs of reading exceed the expected benefits of ignorance (rational ignorance).[58] Some authors have estimated that it would take every user 76 days per year to entirely read the relevant privacy policies, resulting in an overall cost of 781 billion USD.[59] Consequently, users might simply rely on courts to assess the validity of privacy policies, which eventually further decreases incentives of users to read privacy policies and hampers informed consent.

32 The new EU privacy regime does not solve the problem of information asymmetries. Art. 12 § 1 EU-GDPR requires companies to provide information to users "in a concise, transparent, intelligible and easily accessible form, using clear and plain language". However, it is difficult to imagine how these transparency requirements could reasonably be met under a regime that also sets high quantitative thresholds with respect to information for users. In principle, Art. 14 EU-GDPR requires information about: the identity and the contact details of the controller; the contact details of the data protection officer; the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; the categories of personal data concerned; the recipients or categories of recipients of the personal data; the intention to transfer personal data to a recipient in a third country or an international organization; the period for which the personal data will be stored; the legitimate interests pursued by the controller or by a third party; the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability; the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; the right to lodge a complaint with a supervisory authority; the source the personal data originates from and whether it came from publicly accessible sources; the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such

53 *Acquisti/Grossklags*, Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting, in: Camp/Lewis (Ed.), The Economics of Information Security, 2004, 165.

54 *Tsai et al.*, The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, Information Systems Research 22 (2011), 254.

55 *Acquisti/Taylor/Wagman*, The Economics of Privacy, Journal of Economic Literature 54 (2016), 442 (476-478); *Adjerid/Soman/Acquisti*, A Query-Theory Perspective of Privacy Decision Making, Journal of Legal Studies 45 (2016), S97.

56 *Bakos/Marotta-Wurgler/Trossen*, Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts, Journal of Legal Studies 43 (2014), 1.

57 7,500 Online Shoppers Unknowingly Sold Their Souls, April 15, 2010, <http://www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls.html>: „By placing an order via this Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant Us a non transferable option to claim, for now and for ever more, your immortal soul. Should We wish to exercise this option, you agree to surrender your immortal soul [...]".

58 *Ben-Shahar/Schneider*, The Failure of Mandated Disclosure, University of Pennsylvania Law Review 159 (2011), 647; *Wilkinson-Ryan*, A Psychological Account of Consent to Fine Print, Iowa Law Review 99 (2014), 1745.

59 *McDonald/Cranor*, The Cost of Reading Privacy Policies, I/S: A Journal of Law and Privacy for the Information Society 4 (2008), 540.

processing for the data subject. This kind of notice policy is likely to facilitate the exploitation of two effects: attribute substitution and limited attention spans.

33 On the one hand, empirical evidence suggests that users confronted with lengthy privacy policies have a tendency to use cognitive rules of thumb (heuristics) when making their privacy choices. When the relevant information is not available due to a lack of transparency or high transactions costs, users tend to rely on available information and use it as a substitute for the unavailable information (attribute substitution). Such heuristics may sometimes improve decision making.[60] In the field of privacy however, heuristics seem to impair the quality of choices. Empirical evidence shows that privacy policies are often interpreted as a cue signaling a high level of privacy protection regardless of their content.[61] Similarly, users tend to interpret privacy seals as a guarantee of confidential communication,[62] and ignore salient warnings about dangerous malware when downloading software.[63] Invoking formal privacy policies however, can also reduce trust in the company.[64] This shows that privacy policies are likely to trigger effects that run counter to their regulatory objectives.

34 On the other hand, lengthy privacy policies and large quantities of information increase the complexity of privacy choices. The more information a user is confronted with, the more difficult it becomes to select the relevant information (*information overload*) and make a truly informed but 'frugal' choice. Whether consent is given in light of relevant information, heavily depends on the *cognitive load*, i.e. the level of cognitive effort required by the working memory. Short distractions (a couple of seconds) after presenting a privacy policy significantly lower the perception of risks thereby increasing the propensity to give consent.[65] Limited attention spans provide a further plausible explanation for the ineffectiveness of lengthy privacy policies, especially when user attention is focused on the content features of the service and not its privacy features.

35 At first sight, these findings prompt the conclusion that reducing information, simplifying information formats, and forcing users to focus on privacy policies might improve privacy choices.[66] But again empirical evidence shows that reducing complexity is itself a complex endeavor. Information presented as a 'privacy nutrition label' or in a short table format with clearly structured information seems to facilitate the correct assessment of the level of privacy protection as compared to full-text formats.[67] However, even when confronted with table formats, users have difficulties altering default options in a way that reflects their stated privacy preferences.[68] In a similar vein, a more recent study shows that warning boxes that alert users about the worst-case scenario do not have a significant effect on the comprehension of privacy losses and the propensity to share personal information.[69]

36 In general, providing information to users seems to have a limited impact on privacy choices. The warning effect seems to be particularly weak when the incentives to give consent are salient. A study investigating the effects of monetizing personal information on a duopolistic market shows that a privacy-friendly company has a significantly higher market share (83%) than a privacy-unfriendly company if the information about the level of data protection is salient.[70] Once the privacy-unfriendly company offers a 50 cent discount, the market share of the privacy-friendly company shrinks to between 31 and 13%.[71] These findings are in line with several other studies showing that the willingness to pay for

60 *Gigerenzer/Todd/ABC Research Group*, Simple Heuristics That Make Us Smart (2000); for an investigation of the power of heuristics in the creation and implementation of law *Gigerenzer/Engel (Eds.)*, Heuristics and the Law (2006).

61 *Turow et al.*, The Federal Trade Commission and Consumer Privacy in the Coming Decade, I/S: A Journal of Law and Policy for the Information Society 3 (2008), 723 (730).

62 *Moores*, Do consumers understand the role of privacy seals in e-commerce?, Communications of the ACM 48 (2005), 86; for a recent analysis *Marotta-Wurgler*, Self-Regulation and Competition in Privacy Policies, Journal of Legal Studies 45 (2016), S13 (S17-S30).

63 *Good et al.*, User Choices and Regret: Understanding Users' Decision Process about Consensually Acquired Spyware, I/S: A Journal of Law and Policy for the Information Society 2 (2006), 283 (299).

64 *Martin*, Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online, Journal of Legal Studies 45 (2016), S191.

65 *Adjerid et al.*, Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency, Proceedings of the Ninth Symposium on Usable Privacy and Security, 2013, 1 (9).

66 See generally *Ayres/Schwartz*, The No-Reading Problem in Consumer Contract Law, Stanford Law Review 66 (2014), 545 (580-587).

67 *Kelley et al.*, A "Nutrition Label" for Privacy, Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 2009, 1 (9).

68 *Kelley et al.*, A "Nutrition Label" for Privacy, Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 2009, 1 (10-11).

69 *Ben-Shahar/Chilton*, Simplification of Privacy Disclosures: An Experimental Test, Journal of Legal Studies 45 (2016), S41.

70 *Jentzsch/Preibusch/Harasser*, Study on monetising privacy, An economic model for pricing personal information, Report for the European Network and Information Security Agency, 2012, 1 (34-36).

71 *Jentzsch/Preibusch/Harasser*, Study on monetising privacy, An economic model for pricing personal information, Report for the European Network and Information Security Agency, 2012, 1 (36-37).

privacy is generally very low.[72]

37 Perhaps the more significant conclusion relates to the recent proposal to legally compel companies to offer users the choice between a privacy-unfriendly 'free option' and a privacy-friendly 'paid option'.[73] Such a choice, even when bundled with salient information, is likely to appeal to a minority of privacy-sensitive users who are not better informed through additional information. For the majority of users, the temptation of the 'free option' would probably trump the impact of additional information especially when the language used is vague.[74] In sum, it seems that until now there are no good instruments to mitigate the problem of information asymmetries or react to user over-optimism. As long as the EU-GDPR does not specify the requirements as to information formats – for instance pictograms or *one-pagers* –[75] it is unlikely to enable users to make informed privacy choices.

II. Impact of Framing

38 The framing of consent options has been shown to have a significant impact on privacy choices. Generally, people have a tendency to stick with tracking defaults set by digital platforms.[76] The disclosure of personal information is likely to be the product of status quo bias or lacking awareness of exit options. The European legislator has been aware of this problem. Consequently, the EU-GDPR contains a general principle requiring privacy-protective default options. According to Art. 25 § 2 EU-GDPR, companies "shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed". This *privacy by default* principle "applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility".

39 Nevertheless, it is not clear what *privacy by default* precisely means and to what extent it captures the behavioral problems that users are confronted with. While Recital 32 EU-GDPR specifies that a clear affirmative act "could include ticking a box when visiting an internet website", it also allows any other "statement or conduct which clearly indicates [...] the data subject's acceptance" of the processing of personal information. Only "silence, pre-ticked boxes or inactivity" should not be considered as valid consent. In sum, EU privacy law contains two different consent models: explicit consent and implicit (not tacit) consent. Implicit consent might capture cases where users, for instance, type personal information into a web form that uses the HTML standard or JavaScript and contains a privacy notice stating that any such information will be processed. Each consent model relates to empirical findings in behavioral economics.

40 *Explicit consent* and *privacy by default* raise a number of behavioral problems. The initial allocation of a privacy right or a right to consent has a significant impact on the valuation of privacy and the final allocation of personal information even when transaction costs are very low. Obviously, this is not in line with the predictions of the Coase theorem. Consider a group of people that are provided with a high level of privacy and offered the choice to *accept* 2 USD (willingness to accept) for a lower level of privacy, and a group of people that are provided with a low level of privacy and offered the choice to *pay* 2 USD (willingness to pay) for a higher level of privacy.[77] The fraction of people accepting the offer is significantly higher in the former group than in the latter, which indicates that the willingness to pay for strong privacy is significantly lower than the willingness to accept money for weak privacy.[78] This effect is usually associated with *endowment effects*, i.e. the fact that people have a higher valuation for objects they possess than for objects they do not

72 *Rose*, Data Users versus Data Subjects: Are Consumers Willing to Pay for Property Rights to Personal Information?, Proceedings of the 38th Hawaii International Conference on System Sciences, 2005, 1; *Hann et al.*, Overcoming Online Information Privacy Concerns: An Information Processing Theory Approach, Journal of Management Information Systems 24 (2007), 13 (28); *Carrascal et al.*, Your Browsing Behavior for a Big Mac: Economics of Personal Information Online, Proceedings of the 22nd International Conference on World Wide Web, 2013, 189; *Beresford/Kübler/Preibusch*, Unwillingness to pay for privacy: A field experiment, Economics Letters 117 (2012), 25.

73 For a brief discussion *Borgesius*, Behavioural Sciences and the Regulation of Privacy on the Internet, in Alemanno/Sibony (Eds.), Nudge and the Law: A European Perspective (2015), 179 (201-202).

74 For an assessment of vagueness see *Reidenberg et al.*, Ambiguity in Privacy Policies and the Impact of Regulation, Journal of Legal Studies 45 (2016), S163.

75 A condensed information format (one-pager) has been proposed on the German 2015 IT summit in cooperation with the Federal Ministry of Justice and Consumer Protection (<http://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2015/11192915_Vorstellung_OnePager.html>).

76 *Sunstein*, The Storrs Lectures: Behavioral Economics and Paternalism, Yale Law Journal 122 (2013), 1826 (1893).

77 *Acquisti/John/Loewenstein*, What Is Privacy Worth?, Journal of Legal Studies 42 (2013), 249 (260-262).

78 *Acquisti/John/Loewenstein*, What Is Privacy Worth?, Journal of Legal Studies 42 (2013), 249 (264-268). The results suggest that this effect (WTA-WTP ratio: 5/1) is stronger than with normal goods (WTA-WTP ratio: 2,5/1). See also *Grossklags/Acquisti*, When 25 cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information, Proceedings of the Sixth Workshop on the Economics of Information Security (WEIS 2007), 1.

possess.[79] A related explanation builds on *prospect theory* and states that losses loom larger than equal gains (*loss aversion*), even when no risk is involved.[80]

41 The analysis becomes slightly more complicated when considering the design of choice frames without strong monetary incentives. Consider the case in which users are presented either with the option *"I would like to benefit from targeting. I give my consent...☐"* or the option *"I would like to refuse targeting. I do not give my consent...☐"*. While the former is framed as an opt-in (*gains frame*), the latter is framed as opt-out (*loss frame*). Empirical evidence suggests that the willingness to give consent is significantly higher with an opt-out than with an opt-in in similar cases.[81] This effect, however, changes when users are presented with the same options – the only difference being that the respective box is pre-ticked: *"...☑"*. In this case, consent rates are relatively similar across both reverse default options and take an intermediate value between those yielded by the regular default options.[82] A possible explanation is that pre-ticked boxes raise people's awareness that a choice is being made and that they should actively think about whether to stick with the status quo. Assuming that these results can be generalized, the EU-GDPR seems to have found a decent solution to the behavioral problems of default options with respect to consent. However, some problems remain.

42 First, it is not clear whether and to what extent *privacy by default* and the prohibition of pre-ticked boxes apply to other privacy choices than consent, such as the withdrawal of consent or deletion. As it seems, companies may well be allowed to use loss frames and pre-ticked boxes in the design of withdrawal options (*"I do not withdraw my consent...☐"* or *"...☑"*). Companies could use these loopholes to lower withdrawal rates and use confusing default options once consent has been given. Instead of primarily regulating choices over the initial collection of personal information (i.e. consent), it would probably make sense if EU privacy law held a stronger grip on choices over downstream uses. This may become particularly important for Big Data analytics. In some cases, Big Data analytics can generate personal information that did not exist when the user gave their consent. Some users will not want the newly generated information to be used, whereas some of them would not have given their consent initially had they known that Big Data analytics would generate this piece of information out of an innocuous piece of information. Downstream control like withdrawal and deletion then becomes crucial. In a similar vein, a strict implementation of *privacy by default* sets an incentive for companies to engage in more aggressive data gathering strategies, for instance extending the scope of processing purposes. Somewhat relaxing the requirements for initial consent and requiring a specific and properly framed consent renewal for the use of newly generated personal information might mitigate this problem to a certain extent.

43 Second, the problem of most investigations of default options is that they do not consider the effects of cumulative choice options. Digital platforms collect all kinds of personal information for a variety of purposes. This entails a high number of choice options. Some time ago, Facebook allegedly offered users up to 50 settings with 170 choice options scattered all over the network.[83] The higher the number of control options and default rules, the more time consuming and costly it becomes for users to think about these options and change them. An extensive scope of *privacy by default* might therefore lead to a situation where defaults have the same effects as an unchangeable fixed option. This becomes a problem when the bulk of default settings contain options set in a way that do not reflect users' privacy preferences. Furthermore, a high number of default options might also make it difficult to assess how defaults should be altered. Empirical evidence suggests that users have difficulties understanding the meaning of an opt-out (that stops tracking or targeted ads), which eventually induces them to opt-out even though it does not reflect their true privacy preferences.[84] Privacy-sensitive users have been shown to set defaults to delete cookies and thereby also delete opt-out cookies, thus diminishing their level of privacy protection instead of increasing it.[85] This shows that providing users with granular

79 *Kahneman/Knetsch/Thaler*, Experimental Tests of the Endowment Effect and the Coase Theorem, Journal of Political Economy 98 (1990), 1325; *Kahneman/Knetsch/Thaler*, Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias, Journal of Economic Perspectives 5 (1991), 193; *Plott/Zeiler*, The Willingness to Pay-Willingness to Accept Gap, the „Endowment Effect", Subject Misconceptions, and Experimental Procedures for Eliciting Valuations, American Economic Review 95 (2005), 530.

80 *Kahneman/Tversky*, Prospect Theory: An Analysis of Decision Under Risk, Econometrica 47 (1979), 263; *Tversky/Kahneman*, Loss Aversion in Riskless Choice: A Reference-Dependent Model, Quarterly Journal of Economics 106 (1991), 1039 (1047); for a critical summary see *Barberis*, Thirty Years of Prospect Theory in Economics: A Review and Assessment, Journal of Economic Perspectives 27 (2013), 173.

81 *Johnson/Bellman/Lohse, Defaults*, Framing, and Privacy: Why Opting In-Opting Out, Marketing Letters 13 (2002), 5 (7) (opt-out: 96.3 % consent rate / opt-in: 48.2 % consent rate).

82 *Johnson/Bellman/Lohse, Defaults*, Framing, and Privacy: Why Opting In-Opting Out, Marketing Letters 13 (2002), 5 (9) (around 70 % consent rate).

83 *Tucker*, Social Networks, Personalized Advertising, and Privacy Controls, Journal of Marketing Research 51 (2014), 546 (549).

84 *Leon et al.*, Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising, CHI 2012, 1 (1).

85 *Leon et al.*, Why Johnny Can't Opt Out: A Usability Evaluation

control through an extensive use of default options is likely to backfire.

44 Some of these behavioral problems could be solved through the use of technical privacy assistants or privacy bots that help users with default configurations for different types of personal information. These assistants might offer a few general settings (for average users) and a range of more specific settings (for more sophisticated users) that would eventually be applied to all services – browsers, search engines and platforms – and hence reduce the burden of opt-in choices. Without such a technological solution, *privacy by default* would require consent before the use of each single service on a case-by-case basis. This would increase the cost of the consent procedure and eventually deter users from making a deliberate privacy choice in every single case.

45 Third, privacy-protective default options could have drawbacks on the level of competition. On the one hand, privacy-protective defaults and restrictions of information flows in general might create incentives for firms to merge or build technological barriers against switching to facilitate the exchange of information within the firm or lock-in users.[86] This is not an insurmountable problem per se because competition authorities can assess these effects in their merger control procedures. However in the past, competition authorities like the European Commission have been reluctant to operate an in-depth analysis of the interaction between privacy and the level of competition in these procedures, like the *Google/DoubleClick* merger.[87] On the other hand, privacy-protective defaults might preclude small or specialized services from entering the market and bolster the position of incumbent generalist services (GoogleNews, Visa).[88] This in turn might bolster the position of generalist services and deprive users of higher-quality services. These findings prompt the conclusion that reducing the cost of consent through a single interface of privacy settings for every service used (a kind of 'flat privacy option') and somewhat relaxing the requirement of case-by-case ex ante consent might actually foster competition and increase the level of privacy.

46 The protection of privacy becomes even thornier in case of *implicit consent*. Under the rational choice paradigm, users should minimize the time spent on and the risks associated with the disclosure of personal information. Recent findings cast doubt on this hypothesis and show that users willingly provide personal information even when doing so is optional.[89] However, this over-disclosure effect seems to be weaker when companies additionally require some types of personal information through mandatory fields. Voluntary over-disclosure might be driven by social norms (visibility of other users' disclosure behavior), reciprocity towards the service and monetary rewards. This indicates that companies might have an incentive not to condition the use of their service on consent. Instead they might simply make consent optional, increase the visibility of other users' behavior and set incentives for disclosure, thereby escaping the prohibition enshrined in Art. 7 § 4 EU-GDPR and maximizing the inflow of personal information. Implicit consent is likely to be the prime channel for information disclosure, but the EU-GDPR says very little about how to mitigate the awareness and attention problems that might be associated with implicit choice.

III. Impact of Time

47 One of the least understood factors that might influence users' privacy choices and explain the privacy paradox is time. Generally, behavioral economics shows that people are subject to bounded willpower when making intertemporal choices.[90] This means that people have a tendency to procrastinate and opt for immediate benefits. For instance, many people prefer a payment of 110 Euros 'a year and a week from now' over a payment of 100 Euros 'a year from now', while favoring a payment of 100 Euros 'now' over a payment of 110 Euros 'a week from now'.[91] While this kind of present bias or myopia is

of Tools to Limit Online Behavioral Advertising, CHI 2012, 1 (9).

86 See *Picker*, Competition and Privacy in Web 2.0 and the Cloud, Northwestern University Law Review Colloquy 103 (2008), 1 (10).

87 Commission decision of 11/03/2008 declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement (Case No COMP/M.4731 – Google/ DoubleClick), C(2008) 927 final; see also *Edwards*, Stepping Up to the Plate: the Google-DoubleClick Merger and the Role of the Federal Trade Commission in Protecting Online Data Privacy, Working Paper (2008), 1 (<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370734>); *Rodrigues*, Privacy on Social Networks: Norms, Markets, and Natural Monopoly, in: Levmore/Nussbaum (Eds.), The Offensive Internet, 2010, 237.

88 *Campbell/Goldfarb/Tucker*, Privacy Regulation and Market Structure, Journal of Economics & Management Strategy 24 (2015), 47 (48).

89 *Preibusch/Krol/Beresford*, The Privacy Economics of Voluntary Over-disclosure in Web Forms, in Böhme (Ed.), The Economics of Information Security and Privacy (2013), 183 (203).

90 *O'Donoghue/Rabin*, The Economics of Immediate Gratification, Journal of Behavioral Decision Making 13 (2000), 233; *O'Donoghue/Rabin*, Choice and Procrastination, Quarterly Journal of Economics 116 (2001), 121.

91 *Frederick/Loewenstein/O'Donoghue*, Time Discounting and Time Preference: A Critical Review, Journal of Economic

captured by models of hyperbolic discounting, it is not entirely clear whether it really results from a distortion of preferences and what the underlying psychological processes are. The debate about utility functions notwithstanding, the model helps explain several phenomena of self-harming over-consumption; for instance when people overuse their credit card at the beginning of the month or when they eat more fast food than healthy meals.[92] In a similar vein, empirical evidence suggests that users tend to underestimate the long-term risks associated with the disclosure of personal information.[93]

48 Three general tendencies are likely to be observed. First, the longer the time period between consent and the use of personal information, the less likely it is that the user will have considered the risk when consenting. Second, the stronger and the more immediate the rewards from consent, the stronger the underestimation effect. Third, the more intangible the consequences of the use of personal information, the stronger the underestimation effect.[94] These factors might even push people to alter privacy-protective default options and eventually curb the impact of *privacy by default*.[95] More importantly, models of hyperbolic discounting help us to understand how companies might try to exploit myopia to extract more personal information through minimal rewards for consent.

49 The problem becomes clear when comparing a service offering a privacy-unfriendly 'consent option' and a privacy-friendly 'paid option' in a simple model.[96] Suppose that the price for the paid option remains constant over time and that the user only uses one service, maybe due to lock-in effects. Assume that the price of the service over two periods is $p_{paid} = p_{t1} + p_{t2}$, where t1 denotes the point of time when the user begins using the service and t2 denotes some posterior point of time when the service is actually used. Now suppose that the service can extract higher rents from users through *behavioral targeting* but that this practice requires consent to the processing of personal information. The potential to extract a higher rent later on allows the company to lower the price in the first period. It might set $p_{consent} = p_{t1} - c + p_{t2} + \delta p_a$, where p_a denotes the price increase in the second period, c the monetary discount for consent and δ the bias resulting from hyperbolic discounting. If users underestimate p_a because of their cognitive bias, they might think that the consent option is cheaper than the paid option. This is the case if $p_{t1} - c + p_{t2} + \delta p_a \leq p_{t1} + p_{t2}$.

50 The company will then offer users a discount $c \geq \delta p_a$ for giving their consent. The stronger the error, the higher the discount that companies can offer their users. This simple analysis shows that the perception of the service as being 'free' will often be an illusion. More importantly, it shows that assessing consent only makes sense when considering the extent to which personal information may be used to extract user rents in later periods. This will depend on the purposes of data processing. Allowing the processing of personal information for the purpose of the 'analysis of Big Data' is not only conceptually circular. Unspecified purposes are likely to facilitate the exploitation of biases in general and myopia in particular.

51 In light of these findings, behavioral economists tend to conclude that over long time horizons, i.e. if people have to anticipate the long-term costs and risks of their choices in the present, they often fail to make choices that reflect their true preferences and impose externalities on their future selves (*internalities*).[97] Turning positive analysis into a normative conclusion, some authors claim that this constitutes a kind of *behavioral market failure* justifying government interventions.[98] The problem is that until now there is no firm reason why we could or should assume a superior second-order preference of the future self over the present self and hence restrict choices in the present.[99]

Literature 40 (2002), 351 (361). Hyperbolic discounting does not necessarily coincide with a reversal of preferences as described in my example.

92 *Jolls*, Behavioral Law and Economics, in Diamond/Vartiainen (Eds.), Behavioral Law and Economics and Its Applications (2007), 115 (124-125).

93 *Acquisti/Grossklags*, Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting, in Camp/Lewis (Eds.), The Economics of Information Security (2004), 165; *Strandburg*, Social Norms, Self Control, and Privacy in the Online World, in Strandburg/Raicu (Eds.), Privacy and Technologies of Identity: A Cross-disciplinary Conversation, 2006, 31 (39).

94 For the general mechanism see *Rick/Loewenstein*, Intangibility in intertemporal choice, Philosophical Transactions of the Royal Society 363 (2008), 3813.

95 For an assessment in context see *Willis*, When Nudges Fail: Slippery Defaults, University of Chicago Law Review 80 (2013), 1155 (1216-1217).

96 The following thoughts have a flavor of the more complex models discussed by *Gabaix/Laibson*, Shrouded Attributes, Consumer Myopia, and Information Suppression in Competitive Markets, Quarterly Journal of Economics 121 (2006), 505 (512); *Bar-Gill*, Bundling and Consumer Misperception, University of Chicago Law Review 73 (2006), 33 (39–46); *Bar-Gill*, The Behavioral Economics of Consumer Contracts, Minnesota Law Review 92 (2008), 749 (774).

97 *Herrnstein et al.*, Utility Maximization and Melioration: Internalities in Individual Choice, Journal of Behavioral Decision Making 6 (1993), 149 ff.; *Loewenstein/Haisley*, The Economist as Therapist: Methodological Ramifications of "Light" Paternalism, in Caplin/Schotter (Eds.), The Foundations of Positive and Normative Economics: A Handbook, 2008, 210 (212).

98 *Sunstein*, The Storrs Lectures: Behavioral Economics and Paternalism, Yale Law Journal 122 (2013), 1826 (1842 sq.).

99 *Rizzo/Whitman*, Little Brother Is Watching You: New

52 Does this mean that privacy law should ignore users' tendency to opt for immediate rewards and give their consent? I do not believe so. Privacy law could take account of myopia without resorting to outright paternalism.

53 On the one hand, privacy lawyers could implement some of the interpretive rules known from contract law. Long time horizons might justify the application of the *ambiguity rule* enshrined in § 305c II of the German Civil Code. According to this interpretive rule, a provision in a standard form contract is considered invalid when there are doubts about its exact content and meaning (*interpretatio contra proferentem*). A similar rule could be applied when interpreting consent or contract terms on consent.

54 The primary effect of such an interpretive rule would be to increase the burden of proof that companies already carry under Art. 7 § 1 EU-GDPR. Furthermore, it would compel companies to seek consent renewal after longer time periods.

55 On the other hand, privacy law could try to mitigate the problem of myopia through cooling-off periods. Consent options could be designed such that users have to reconsider their opt-in after the initial opt-in. § 7 II of the German Law on Unfair Commercial Practices, for instance, requires a *double opt-in* (DOI) when consenting to commercial ads. In this case, consent is only valid if the user opts in twice, the second opt-in usually being given through a clickbox in an email that confirms that the user has previously opted in (combination of two opt-in defaults). Another solution could be to require a *confirmed opt-in* (COI). In this case, consent would only be valid if the user does not opt out after being reminded that she has previously opted in (combination of an opt-in and an opt-out default). Finally, an intermediate solution could be to use a pre-ticked box for the second choice to be made. Since DOI and COI would generally increase protection of users, the use of pre-ticked boxes would probably not be prohibited by Recital 32 EU-GDPR.

IV. Impact of Control

56 The general approach of EU privacy law is to provide users with rights to control the various steps of the processing of personal information – like consent to processing (Art. 7 § 1 EU-GDPR), withdrawal of consent (Art. 7 § 3 EU-GDPR), access to data (Art. 15 EU-GDPR), rectification of data (Art. 16 EU-GDPR), deletion of data (Art. 17 EU-GDPR), restriction of processing (Art. 18 EU-GDPR), portability of data (Art. 20 EU-GDPR) or objection to processing (Art. 21 EU-GDPR). On a deontological view, control might be considered as a precept of autonomy and the fundamental right to data protection under Art. 8 of the EU Charter of Fundamental Rights. However on a consequentialist view, control might trigger behaviors that are incompatible with the objectives of user empowerment through rights.

57 Generally, psychological evidence shows that control over some risks associated with an activity might induce users to neglect or underestimate other risks resulting from the same activity, thus creating an illusion of control.[100] Similar problems may arise when increasing control over single steps of the processing of personal information. Empirical evidence suggests that increasing the degree of control over the release of personal information may induce users to underestimate the risks associated with the use of personal information.[101] In a similar vein, a recent field study shows that facilitating the use of the privacy control interface on Facebook and increasing control over the type of personal information and third-party tracking significantly increases the propensity to share personal information.[102] The upshot of these findings is that rights to control are ambiguous tools.

58 If the objective of such rights is to facilitate the objective level of control, this objective will probably be achieved – especially for sophisticated users. If, however, the objective is to improve the matching of true privacy preferences and objective privacy risks, control rights might have effects that run counter to these objectives. In social networks, there is a risk that users might confound control vis-à-vis other users and control vis-à-vis the company. Giving users control over the visibility of personal information for other users might trigger the illusion that they are not being tracked by the company either. In sum, making control options more granular will not only increase the costs of privacy choices; it also has the potential to mislead users and impair the quality of privacy choices. How could EU privacy law guarantee a sound level of granularity of control without disempowering users?

Paternalism on the Slippery Slopes, Arizona Law Review 51 (2009), 685 (701); in the context of privacy law *Jolls*, Rationality and Consent in Privacy Law, Working Paper, 2010, 1 (51).

100 *Peltzman*, The Effects of Automobile Safety Regulation, Journal of Political Economy 83 (1975), 677; for a metastudy *Klein/Helweg-Larsen*, Perceived Control and the Optimistic Bias: A Meta-Analytic Review, Psychology and Health 17 (2002), 437.

101 *Brandimarte/Acquisti/Loewenstein*, Misplaced Confidences: Privacy and the Control Paradox, Social Psychological and Personality Science 4 (2013), 340.

102 *Tucker*, Social Networks, Personalized Advertising, and Privacy Controls, Journal of Marketing Research 51 (2014), 546.

59 One possibility could be the use of technical user assistants or privacy bots based on artificial intelligence and smart (personalized) defaults.[103] Big Data analytics and artificial intelligence could be used to generate information about users' privacy preferences and design technical user assistants and default rules tailored to these preferences – just like targeted ads are tailored to consumption preferences. These assistants or defaults would require a one-time (mandated) active choice for specific types of services and data and then learn from users' past choices. The advantage is that the initial setup of the assistant or default would require full user awareness and then allow for granular control without having to make an active choice each and every time. This would reduce the costs of privacy choices.

60 The obvious disadvantage is that such assistants or defaults would be quite intrusive and require the processing of personal information.[104] Furthermore, users might become entrenched in their past privacy choices which might become a problem when the assistant or default determines the kind of information that users are exposed to, for instance in a social network. This might eventually lead to filter bubbles or echo chambers.[105] Finally, alleviating users from the burden of choice might undermine learning and hamper the emergence of new tastes and preferences. To a certain extent, these problems could be solved through limited data retention periods and the renewal of privacy settings on a regular basis. Choice renewals would compel users to start with a clean slate, thereby limiting the effects of status quo bias and raise users' awareness. To conclude, personalized technical assistants and defaults are not a panacea, but it is difficult to see how control could really work out in practice without any kind of technical assistance.

D. Behavioral Privacy Law and the Problem of 'Mixed Rationalities'

61 Some authors have suggested that the legislator could or should nudge users towards disclosing less personal information.[106] Others have seen nudges as a threat to privacy.[107] Moreover, some lawyers have qualified the prohibition principle enshrined in Art. 6 § 1 EU-GDPR as straightforward 'interventionist paternalism' and *privacy by default* enshrined in Art. 25 § 2 EU-GDPR as 'libertarian paternalism' and hence a paternalistic nudge.[108] These claims notwithstanding, the understanding of nudges is rather vague.[109] According to the proponents of libertarian paternalism, a nudge describes any kind of intervention affecting "the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid."[110] Other authors have taken a broader approach to libertarian paternalism as a set of interventions designed to overcome unavoidable cognitive biases to approximate autonomous choices under idealized conditions.[111] One of the problems of the nudging debate is that the *objectives* and *effects* of regulatory tools are often swept under the rug. In addition, there is usually no precise discussion about how the objectives and effects of nudges are or should be related. Consequently, all kinds of regulatory tools and interventions are considered as nudges, even when neither their goals nor their effects are really clear. This translates into a legal problem when determining the grounds on which the intervention may be justified.

62 Consider default options in privacy law. Without any further specification of the objective and effects of a default rule, it does not make sense to qualify a default option as a nudge. As I have shown above, an opt-in default may be justified on different legal grounds.

63 If the purpose of an opt-in default is to set a strategic incentive for companies to disclose better information for users, it aims at reducing information asymmetries and hence a market failure. Similarly,

103 *Sunstein*, Deciding by Default, University of Pennsylvania Law Review 162 (2013), 1; *Porat/Strahilevitz*, Personalizing Default Rules and Disclosure with Big Data, 112 Michigan Law Review 112 (2014), 1417; *Sunstein*, Choosing Not to Choose (2015), 157-173.

104 *Porat/Strahilevitz*, Personalizing Default Rules and Disclosure with Big Data, 112 Michigan Law Review 112 (2014), 1417 (1467-1469); *Sunstein*, Choosing Not to Choose (2015), 169-173.

105 See *Pariser*, The Filter Bubble: How the New Personalized Web is Changing What We Read and How We Think (2012).

106 *Acquisti*, Nudging Privacy: The Behavioral Economics of Personal Information, IEEE Security & Privacy, November/December 2009, 82; *Balebako et al.*, Nudging Users Towards Privacy on Mobile Devices, CHI 2011, 1; *Wang et al.*, Privacy Nudges for Social Media: An Exploratory Facebook Study, PSOSM 2013, 1; *Wang et al.*, A Field Trial of Privacy Nudges for Facebook, CHI 2014, 1; *Ziegeldorf et al.*, Comparison-based Privacy: Nudging Privacy in Social Media (2015), 1.

107 *Kapsner/Sandfuchs*, Nudging as a threat to privacy, Review of Philosophy and Psychology 6 (2015), 455.

108 *Krönke*, Datenpaternalismus. Staatliche Interventionen im Online-Datenverkehr zwischen Privaten, dargestellt am Beispiel der Datenschutz-Grundverordnung, Der Staat 55 (2016), 319 (325-330).

109 *Dworkin*, Paternalism, in Zalta et al. (Eds.), Stanford Encyclopaedia of Philosophy Online, 2016 (<https://plato.stanford.edu/entries/paternalism/>).

110 *Sunstein/Thaler*, Nudge: Improving Decisions About Health, Wealth, and Happiness (2008), 6.

111 *Rebonato*, Taking Liberties: A Critical Examination of Libertarian Paternalism (2012), 6.

an opt-in default could be used to mitigate collective action problems and the negative externalities associated with an unconstrained disclosure of personal information. The prime purpose of such a default would not be to protect users against themselves but to enhance the efficiency of contracts between companies and users. In both cases, it would not make much sense to qualify the default option as a paternalistic nudge, since the default rule could more aptly be justified within the standard economic framework and the traditional approach to market failures.

64 However, if the purpose of an opt-in default is to correct the effects of over-optimism and exploit users' status quo bias, it aims at correcting supposedly distorted privacy preferences or at helping users to avoid individual mistakes, i.e. violations of the axioms posited by rational choice theory. Its prime purpose would be to protect users against mistaken privacy choices. It would then be a nudge in the sense of libertarian paternalism.

65 More generally, this shows that not every type of privacy regulation informed by behavioral economics can reasonably be qualified as a paternalistic nudge. Sometimes, an intervention that seems to be justified on the grounds of libertarian paternalism at first sight might well be justified as a correction of a market failure within the standard economic framework. Simply put, it might make sense to increase the depth of the legal 'duck test' when determining whether an intervention actually is a paternalistic nudge and how the intervention may be justified legally.[112] An intervention may look like a paternalistic nudge (look like a duck), but it might not pursue the objectives or have the effects of a paternalistic nudge (walk, swim and quack like a duck). Therefore, it is crucial to draw a sharper distinction between *libertarian paternalistic regulation* and *non-paternalistic soft regulation*.[113]

66 The law offers various doctrinal frameworks to implement this distinction, most notably the principle of proportionality. According to this principle, a government intervention is justified if it pursues a legitimate objective, if it is suitable and necessary to achieve this objective, and if the costs of the intervention – the weight of the infringement of an individual right – are not disproportionate to its benefits (balancing test).[114]

67 The assessment of the *legitimate objective* is purely normative. The legislator has discretionary powers in determining these objectives but there is a large consensus that the protection of the public interest is easier to justify than outright paternalism.[115] The correlate of discretion is the constitutional duty to specify and justify the objectives. Some of the normative misunderstandings could be solved if the rules of privacy law specified whether an intervention aims at protecting users against themselves (paternalism) or at correcting a market failure (public interest).[116] A nudge used to correct a market failure resulting from unfettered consent should be easier to justify than a nudge to protect against mere harm to the self.

68 The *suitability test* requires an empirical assessment of facts. The suitability threshold is rather low and met if the intervention potentially furthers the legitimate objective. On this level of the test, the assessment might draw a distinction between interventions that mainly correct biases (*debiasing*) and those that mainly reinforce existing cognitive biases for the regulatory objective (*rebiasing*).[117] In general, interventions based on the behavioral insights presented in the previous sections will potentially generate the intended effect. Behavioral insights, for instance about the unintended consequences of too much information or control, could be used to somewhat increase the depth of the suitability test and hence the burden of justification imposed on regulators.

69 The *necessity test* can be considered as a legal implementation of pareto-optimality.[118] The

112 The 'duck test' is often phrased as follows: "This bird has no label that says 'duck'. But the bird certainly looks like a duck. Also, he goes to the pond and you notice that he swims like a duck. Then he opens his beak and quacks like a duck. Well, by this time you have probably reached the conclusion that the bird is a duck, whether he's wearing a label or not." The origin of the phrase is not clear but often attributed to US ambassador Richard Cunningham Patterson Jr., see *Immerman*, The CIA in Guatemala: The Foreign Policy of Intervention (1982), 102.

113 *Sunstein*, The Ethics of Nudging, Yale Journal on Regulation 32 (2015), 413 (426), distinguishes between *paternalistic nudges* and *market failure nudges*.

114 *Harbo*, The Function of the Proportionality Principle in EU Law, European Law Journal 16 (2010), 158 (165).

115 *Schweizer*, Chapter 7: Nudging and the Principle of Proportionality, in Mathis/Tor (Eds.), Nudging – Possibilities, Limitations and Applications in European Law and Economics (2016), 93 (102-106).

116 *Dworkin*, Paternalism, in Zalta et al. (Eds.), Stanford Encyclopaedia of Philosophy Online, 2016 (<https://plato.stanford.edu/entries/paternalism/>).

117 *Larrick*, Chapter 16: Debiasing, in Koehler/Harvey (Eds.), Blackwell Handbook of Judgment and Decision Making (2004), 316; *Soman/Liu*, Debiasing or rebiasing? Moderating the illusion of delayed incentives, Journal of Economic Psychology 32 (2011), 307 (309), define *rebiasing* as the use of a second bias to offset the effects of the original bias while achieving the same result as *debiasing*. On a legal view, however, there could be cases where the regulatory purpose of *rebiasing* would be distinct from that of *debiasing*.

118 *Alexy*, A Theory of Constitutional Rights (2002), 66-69; *Petersen*, How to Compare the Length of Lines to the Weight of Stones: Balancing and the Resolution of Value Conflicts in Constitutional Law, German Law Journal 14 (2013), 1387

threshold is met if the least restrictive (coercive) but equally effective means of achieving the objective is implemented. Nudges or soft regulation will usually be the least coercive means with the potential to be as effective as outright coercion. Notably, the effect of default options is not weaker when people are told that the chosen default is usually effective.[119] Therefore, soft interventions need not be subliminal; they can and should be transparent and be subject to judicial scrutiny.[120] Perhaps the most important consideration is that designing effective nudges will often be complex and costly.[121] Designing privacy-protective default options, for instance, requires very granular regulation capturing the details of choice frames. The crucial question is whether the freedom benefits of such a legal nudging framework will really outweigh its costs. This should be assessed in the *balancing prong* of the proportionality principle, where the scales could be tilted against soft regulation in favor of traditional regulation in a surprisingly large number of cases.

E. Conclusion

70 In this article, I have argued that the legal problems raised by consent and the monetization of personal data cannot be solved without considering how users actually behave. By the same token, I have tried to flesh out some of the 'sweet spots' where privacy law could step in to steer privacy choices. My argument rests on the claim that it is not sufficient to design the rules of privacy law on the grounds of either a standard economics or a behavioral economics analysis. To fully capture the regulatory problems addressed by privacy law, we need both.

71 Looking through the lens of game theory, I have argued that consent will often reflect a rational choice. In networked environments, the protection of privacy has the features of a collective action problem. In this dilemma, consent can be considered as a rational choice yielding a suboptimal level of collective privacy and imposing negative externalities on other users. Looking through the lens of behavioral economics, I have argued that bounded rationality and bounded willpower will often make it difficult for users to make choices according to their stated privacy preferences. While the impact of information is rather low when consent is incentivized, framing, time and control have a strong impact on privacy choices. Companies have an incentive to exploit these effects and take advantage of bounded rationality. However, the combined analysis shows that we should be very cautious when assessing the objectives and effects of what has come to be called a privacy nudge.

72 On the one hand, debiasing users, i.e. facilitating rational choices, could well accelerate the erosion of privacy in environments relying on the use of Big Data. This result casts doubt on the implicit assumption that informing users would push them to disclose less personal information. On the other hand, using privacy-protective nudges to constrain users' propensity to disclose personal information may not only be justified to correct cognitive biases and behavioral market failures. Such restrictions might well be justified to cope with public goods problems and counter negative externalities. In this case, the nudge would not qualify as an intervention on the grounds of *libertarian paternalism* but on the grounds of *non-paternalistic soft regulation*.

73 Accordingly, the scope of libertarian paternalism and nudging in the paternalistic sense might be much smaller in privacy law than the existing literature suggests. Collective action problems in Big Data environments or the privacy externalities associated with unraveling might even justify stricter restrictions, such as sectoral prohibitions. An integrated approach combining competition law, consumer protection law, and data protection law might be the most adequate to address the regulatory problems associated with the continuous monetization of privacy.[122] In the end, behavioral and traditional interventions in privacy law should be used as complements, not substitutes.

(1394).

119 *Loewenstein et al.*, Warning: You are about to be nudged, Behavioral Science & Policy 1(2015), 35.

120 *Sunstein*, The Ethics of Nudging, Yale Journal on Regulation 32 (2015), 413 (428).

121 *Willis*, When Nudges Fail. Slippery Defaults, University of Chicago Law Review 80 (2013), 1155 (1161); *Bubb/Pildes*, How Behavioral Economics Trims Its Sails and Why, Harvard Law Review 127 (2014), 1595.

122 *Kerber*, Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection, GRUR Int. 2016, 639.

Digital Content and Sales or Service contracts under EU Law and Belgian/French Law

by **Hervé Jacquemin**, Professor at the University of Namur, Head of eCommerce Unit – Research Centre on Information, Law and Society (CRIDS), Member of the Brussels Bar

Abstract: The rather novel concept of "digital content" is defined and regulated both in the Consumer Rights Directive and in the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content (dated 9 December 2015). In this paper, the concept is presented, as well as the reasons why the European legislator adopted (or is willing to adopt) protection measures to the benefit of consumers in this context. Relying on this analysis, the paper will further discuss the articulation issues between the notion of "digital content" and other relevant concepts under EU Law and some national laws (of civil Law countries). First, a comparison between the notion of digital content and other concepts used at the EU level (and in the corresponding legal framework adopted in the Member States), in regulations protecting the consumers (the concepts of "goods", "services", "sales" or "services contracts", etc.) will be carried out. The concept will then be compared with the classical notions used in Belgian (and French) Contract Law, especially in the Civil Code ("contract of enterprise", "sales contract", etc.).

Keywords: Digital content; consumer protection; goods; services; sales contract; service contract; articulation issues between concepts; French and Belgian Civil Law

Recommended citation: Hervé Jacquemin, Digital Content and Sales or Service contracts under EU Law and Belgian/French Law, 8 (2017) JIPITEC 27 para 1.

A. Introduction

1 The concept of "digital content" was introduced into the EU legal framework by the directive 2011/83/EU on consumer rights[1] (hereafter, "Consumer Rights Directive"), where it is defined as "data which are produced and supplied in digital form".[2]

2 This definition is broad and, accordingly, the examples of "digital content" are numerous. Some of them are provided by the Recital 19 of the Consumer Rights Directive: "computer programs, applications, games, music, videos or texts, irrespective of whether they are accessed through downloading or streaming, from a tangible medium or through any other means". Social networks, archiving services in the Cloud, or some OTT services (WhatsApp for instance) could also be added.

3 Consumers are increasingly becoming recipients of digital content and, considering that the protection mechanisms already enacted in the sector-specific regulations or in the horizontal regulations protecting consumers are no longer sufficient, some additional legal provisions especially dedicated to digital content (albeit very few) were introduced in the Consumer Rights Directive.[3] Namely: information

1 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, *OJ* L 304, 22.11.2011.

2 Art. 2, 11°, of the Consumer Rights Directive.

3 On the legal measure (to be) enacted in order to protect the consumer of digital content, see F. Coppens, M. Demoulin,

duties, no matter the contract is concluded at a distance, off-premises or face-to-face in a bricks and mortar shop;[4] specific starting point for the withdrawal period;[5] and possible exception from the right of withdrawal.[6]

4 On 9 December 2015, the EU Commission formulated a Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content[7] (hereafter, "the Proposal"). It is an initiative, among many others, delivered by the Commission in the context of its Digital Single Market Strategy,[8] which was launched in May 2015.

5 There are indeed some differences among the Member States with regard to the consumer Contract Law rules applicable to the digital content, especially when it is provided online and across borders. The lack of a clear legal framework and the correlative legal uncertainty for both businesses (that must expose additional costs in order to comply with distinct mandatory rules at the national level) and consumers (suffering from a lack of confidence when buying digital contents) constitutes an obstacle to the growth of electronic commerce in Europe.[9] Following Recital 5 of the Proposal, "in order to remedy these problems, both businesses and consumers should be able to rely on fully harmonised rules for the supply of digital content setting out Union-wide contractual rights which are essential for this type of transaction". Accordingly, the Proposal provides protection rules dealing with the conformity of the digital content with the contract, as well as with the termination and the modification of the contract (including remedies and modalities for the exercise of the rights granted to the consumers).

6 The purpose of the present paper is not to analyse the protection rules lying in the Proposal as such. Instead, it will focus on the concept of "digital content", as defined in the Consumer Rights Directive and in the Proposal, and on the reasons why the European legislator adopted (or is willing to adopt) protection measures to the benefit of consumers in this context. Relying on this analysis, the paper will further discuss the articulation issues between the concept of "digital content" and other relevant concepts under EU Law and some national laws (of civil Law countries). First, a comparison between the concept of digital content and other concepts used at the EU level (and in the corresponding legal framework adopted in the Member States), in regulations protecting the consumers (the concepts of goods, services, sales or services contracts, etc.) will be carried out. The following section then compares the classical concepts used in Belgian (and French) Contract Law, especially in the Civil Code ("contract of enterprise", "sales contract", etc.). The objective is not only theoretical and conceptual as such concepts are indeed the key factors that determine the scope of the legal framework.

B. Concept of "digital content" and purpose of the legal framework protecting consumers

I. Legal definition of "digital content"

1. Broad definition of the digital content under the Proposal

7 Notwithstanding the broad definition already provided by the Consumer Rights Directive (see above), the Proposal includes another definition of the "digital content". It "means (a) data which is produced and supplied in digital form, for example video, audio, applications, digital games and any other software; (b) a service allowing the creation, processing or storage of data in digital form, where such data is provided by the consumer, and (c) a service allowing sharing of and any other interaction with data in digital form provided by other users of the service".[10]

R. Robert et S. Dusollier, *Digital products in the acquis communautaire in the field of consumer protection*, Research study for the BEUC, 2009 ; M. Demoulin, *Droit des contrats à distance et du commerce électronique,* Brussels, Kluwer, 2010, p. 7 *et seq.*; H. Jacquemin, «Digital Content and Consumer Protection within European Law», *Proceedings of the 8th International Workshop for Technical, Economic and Legal Aspectsof Business Models for Virtual Goods,* Namur, PUN, 2010, p. 41 *et seq.*; M.B.M. Loos, N. Helberger, L. Guibault, C. Mak, L. Pessers, J.K. Cseres, B. van der Sloot et R. Tigner, *Comparative analysis, Law and Economics analysis, assessment and recommendations for possible future rules on digital content contracts,* Study of the University of Amsterdam, 2011; U. Stenzel, M. G. S. Lima et J.J. Downes, *Study on Digital Content Products in the EU,* IBF International Consulting for the European Commission, 2012, 86 p.; N. Helberger, M.B.M. Loos, L. Guibault, C. Mak et L. Pessers, «Digital Content Contracts for Consumers», *J. Consum. Policy,* 2013/36, pp. 37-57; H. Jacquemin, "La protection du consommateur de contenus numériques », *D.C.C.R.*, 2015/108-109, p. 5 *et seq.*

4 Art. 5 (1), (g) and (h), and 6 (1), (r) and (s), of the Consumer Rights Directive.

5 Art. 9 (2), (c), of the Consumer Rights Directive.

6 Art. 16 (m) of the Consumer Rights Directive.

7 COM(2015) 634 final.

8 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A Digital Single Market Strategy for Europe", COM(2015) 192 final.

9 See Recitals 1-4 of the Proposal.

10 Art. 2 (1) of the Proposal.

8 *Littera* a) is equivalent to the definition given in the Consumer Rights Directive (see the Introduction above). *Littera* b) and *Littera* c) are new and confirm that the "services" on data shall also be considered as digital content. Pursuant to Recital 11 of the Proposal, "in order to cater for fast technological developments and to maintain the future-proof nature of the notion of digital content, this notion as used in this Directive should be broader than in Directive 2011/83/EU of the European Parliament and of the Council". In that context, and although in my opinion, both services mentioned under b) and c) should normally be included in the definition of digital content under the Consumer Rights Directive, the definition of the Proposal provides a higher level of legal certainty and prevents possible discussion on this point.

9 For the sake of clarity and consistency, the definition of digital content provided in the Consumer Rights Directive should be amended. Otherwise, there will be distinct definitions of a single concept at the EU level and one could contest that services under b) and c) are also subject to the Consumer Rights Directive.

10 Some additional features confirm the broadness of the concept under the Directive and (even more under) the Proposal. First, the distribution channel or the medium used for the transmission are not relevant: no matter whether it is provided online (by streaming, downloading, access to the social media, etc.) or offline, on a tangible medium (on a DVD, CD, Flash Card, USB, etc.).[11] It must however be noted that in the Consumer Rights Directive, protection rules applicable to the digital content are different, depending whether it is supplied on a tangible medium or not (see below). Such a distinction is not made in the Proposal and it must be approved. The Proposal even goes a step further, as the directive shall also apply to "any durable medium incorporating digital content where the durable medium has been used exclusively as a carrier of digital content".[12] The legal framework (and the corresponding protection measures) applicable to the digital content is therefore extended to the medium. In other words, the digital content is the "principal" and the medium, considered as the "accessory", shall be subject to an equivalent legal framework (it is expressed by the old legal proverb "*accessorium sequitur principale*"). This is contradictory to the meaning of the Consumer Rights Directive, where the digital contents supplied on a tangible medium are considered as goods and governed by the legal protection measures applicable to them (see below).

11 Secondly, the digital content shall be subject to an agreement concluded between the supplier and the consumer, and in this context, no matter the counter-performance provided by the consumer – money, personal data or other data. This is very clear in the Proposal, where it is expressly stated.[13] It should also be the case under the Consumer Rights Directive, at least when the digital content is provided online (following the DG Justice Guidance Document issued in June 2014).[14] It shall obviously be approved as soon as the business model of various social networks or platforms (that must be considered as "digital content") is not necessarily built on the price paid in money by the consumers, but on the revenues gained with the processing of their personal data and the advertising.

12 The existence of a "digital content" is a condition *sine qua non* for the application of the Proposal (or the specific provisions of the Consumer Rights Directive using this concept) but is it not the only one (see also the *ratione personae* requirements, for instance). Furthermore, various contracts are excluded from the scope of these regulations as under the Proposal, the directive "shall not apply to contracts shall regarding : (a) services performed with a predominant element of human intervention by the supplier where the digital format is used mainly as a carrier; (b) electronic communication services as defined in Directive 2002/21/EC; (c) healthcare as defined in point (a) of Article 3 of Directive 2011/24/EU; (d) gambling services meaning services which involve wagering a stake with monetary value in games of chance, including those with an element of skill, such as lotteries, casino games, poker games and betting transactions, by electronic means and at the individual request of a recipient of a service; (e) financial services".[15] These exclusions tend to mitigate the consequences resulting from the broadness of the concept of digital content.

13 Finally, it is interesting to point out that under Belgian Law, the concept of "digital content" is not used in the legal provisions (except in the provisions

11 See Recital 11 of the Proposal.

12 Art. 3 (5) of the Proposal (with the exception of Articles 5 and 11).

13 See Article 3 (1) of the Proposal.

14 DG Justice Guidance Document concerning Directive 2011/83/UE of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, June 2014, p. 8 (hereafter the DG Justice Guidance Document): "Contrary to the definition of sales and service contracts, the Directive does not mention 'payment' for the latter two types of contracts. Therefore, it would seem to apply also to contracts for the supply of public utilities and online digital content even if they did not involve payment".

15 See Art. 3 (2) of the Consumer Rights Directive and Art. 3 (5) of the Proposal.

implementing the Consumer Rights Directive[16] and in a single other case).[17] The concepts of immaterial or intangible goods are used much more frequently by the legislator or the judge[18] but it was obviously not the option taken in Consumer Law.

2. Consequences resulting from the use of a broad definition

14 The choice of a broad concept is very positive, if the objective is to ensure that the protection measures shall be observed within a wide range of occurrences. As already mentioned, the number of occurrences could however be limited with the exclusion of numerous contracts from the scope of the regulation (and this is the case in the Proposal). Even in that case, some issues resulting from the potential concomitant application of other regulations shall be addressed; at best, the legal framework will be very complex and therefore not easy to apply, and at worst, some contradictions will need to be resolved.

15 We will discuss some of these issues below; more precisely, the comparison will be made with some concepts consecrated at the EU level in the Unfair Commercial Practices Directive, in the Consumer Rights Directive, and in the directive 1999/44/EC on sales of consumer goods. As soon as various occurrences can be qualified as digital content under the Proposal and as goods, services, products, etc., under these other regulations protecting consumers, various legal provisions shall be observed simultaneously.

16 Some issues could also result from the articulation with the key concepts used in other regulations, not necessarily dedicated to consumer protection[19] and accordingly, the concurrent application of these regulations with the Proposal. Most digital contents are indeed protected under copyright Law; some digital contents could be considered as personal data, protected under the General Data Protection Regulation;[20] digital contents could also be considered as information society services, in the meaning of the directive on electronic commerce,[21] or as audiovisual media services in the meaning of the Audiovisual Media Services Directive;[22] some trust services governed by the eIDAS regulation[23] – electronic signature; electronic time-stamp, etc. – could be qualified as digital contents etc.

II. Weakness of the consumer of digital contents

17 Prior to the adoption of the Consumer Rights Directive, many EU directives were already dedicated to consumer protection.[24] Namely, among others

16 See Book VI and Book XIV of the Belgian Code of Economic Law.

17 Art. 4 of the Decreet of the Flemish Community of 18 March 2011 modifying the Decreet of 13 July 2001 portant stimulation d'une politique culturelle locale qualitative et intégrale, en ce qui concerne la bibliothèque digitale, *Moniteur Belge*, 11 April 2011.

18 See the examples given by P. Lecocq and A. Puttemans, «Rapport belge provisoire – questionnaire relatif au thème n° 1: L'immatériel et les biens», *Journées espagnoles sur l'Immatériel*, Association Henri Capitant des amis de la Culture juridique française, 19-23 May 2014, available <http://www.henricapitant.org/sites/default/files/Belgique_0.pdf>, pp. 3-4.

19 See N. Helberger, M.B.M. Loos, L. Guibault, C. Mak et L. Pessers, «Digital Content Contracts for Consumers», *J. Consum. Policy*, 2013/36, pp. 44 et s.; S. Dusollier, «The relations between copyright law and consumers'rights from a European perspective», note for the European Parliament, 2010, available on <www.ssrn.com/abstract=2127736>; H. Jacquemin, «La régulation de certains aspects juridiques du commerce électronique par les Communautés», report for the Conseil Supérieur de l'Audiovisuel, Brussels, 2011, 73 p., available on <http://www.csa.be/system/documents_files/1659/original/HJACQUEMIN_competence_communautes_commerceFINAL.pdf?1326376554>.

20 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *OJ* L 119, 4 May 2016, p. 1–88. The "information society services" is "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" (Art. 2 (a) of the directive on electronic commerce, which refers to Art. 1 (2) of directive 98/34/EC as amended by Directive 98/48/EC).

21 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *O.J.*, L 178 of 17 July 2000, p. 1-16.

22 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services, *OJ* L 95, 15 April 2010. Audiovisual Media Services means "a) a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union which is under the editorial responsibility of a media service provider and the principal purpose of which is the provision of programmes, in order to inform, entertain or educate, to the general public by electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC. Such an audiovisual media service is either a television broadcast as defined in point (e) of this paragraph or an on-demand audiovisual media service as defined in point (g) of this paragraph ; ii) audiovisual commercial communications" (Art. 1 (1) (a) of the AVMS Directive).

23 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, *OJ* L 257, 28 August 2014.

24 For an overview of Consumer Law within the European

they dealt with: unfair contract terms;[25] unfair commercial practices;[26] and sale of consumer goods and associated guarantees;[27] etc. Some legislative interventions were particularly dedicated to contracts concluded at a *distance* – directive 97/7/EC on distance contracts[28] – and *by electronic means* – directive 2000/31/EC on electronic commerce.[29] Since the adoption of the Consumer Rights Directive in October 2011, most of them have remained applicable (with the exception of directive 97/7/EC, which was repealed). In these directives, the *ratio legis* for the protection measures lies specifically in the weak position of a consumer entering into a relationship with a supplier, a seller or a trader (acting in their commercial or professional capacity).[30] The European Legislator assumes that consumers mainly suffer from a lack of knowledge as regards legal or factual data related to the agreements and do not have the same bargaining power as the other party to the contract.

18 To ensure a high level of protection for consumers, protection rules have been enacted such as: right of withdrawal; information duties; formal requirements; prohibition of unfair contract terms or unfair commercial practices; and conformity requirements and guarantees. The main objectives are to ensure informed consent and to prevent any potential fraud or abuse by the professional of the consumer's inherently weaker position, before the conclusion of, at the moment of, or during the performance of the contract.

19 In the context of digital content, the weakness of the consumer mainly arises out of the object of the contract – a digital content – with the potential lack of knowledge due to the fact that it is a technological item (with issues of interoperability or geo-blocking, for instance). Furthermore, the consumer could be surprised to download an app on their smartphone free of charge, and then to be requested to carry out an integrated purchase, with the payment of a price, in order to benefit from all its functionalities (this is very usual for most games). The consumer could also suffer from a lack of knowledge of their rights, related to the termination of the contract or the portability of their data. Some issues are already addressed by the provisions of the Consumer Rights Directive especially dedicated to digital content (see in particular the information duties). Considering that the current legal framework did not address the other abovementioned weaknesses appropriately, additional protection measures are prescribed by the Proposal.

20 It is also usual that for most digital contents provided to the consumers, the terms and conditions governing their provision can only be accepted or refused (it is a so-called "adhesion contract" – "*contrat d'adhésion*"). The average consumer is therefore the weaker contract party (compared

Union, see H. Schulte-Nölke (ed.), *EC Consumer Law Compendium – Comparative Analysis*, Universität Bielfeld, 2008, 845 p.

25 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, *O.J.*, L 95 of 21 April 1993, p. 29-34 (hereafter, "directive 93/13/EEC on unfair contract terms").

26 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'), *O.J.*, L 149 of 11 June 2005, p. 22-39 (hereafter, "directive 2005/29/EC on unfair commercial practices").

27 Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees, *O.J.*, L 171 of 7 July 1999 (hereafter, "directive 1999/44/EC on sales of consumer goods").

28 Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, *O.J.*, L 144 of 4 June 1997 (hereafter directive 97/7/EC on distance contracts). See also the directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC (*O.J., L 271 of 9 October 2002, p. 16-24) could also be mentioned. In any case, it will not be analysed further (the paper will not focus on digital content that could be considered as financial services).*

29 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *O.J.*, L 178 of 17 July 2000, p. 1-16 (hereafter, "directive 2000/31/EC on electronic commerce").

30 On the weakness of a contractual party, see F. Leclerc, *La protection de la partie faible dans les contrats internationaux (Etude de conflits de loi)*, Brussels, Bruylant, 1995; M. Fontaine, «La protection de la partie faible dans les rapports contractuels (Rapport de synthèse)», J. Ghestin and M. Fontaine (eds), *La protection de la partie faible dans les rapports contractuels. Comparaisons franco-belges,* Paris, L.G.D.J., 1996, p. 616 *et seq.*; Ch. Bourrier, *La faiblesse d'une partie au contrat,* Louvain-la-Neuve, Bruylant, 2003; H. Jacquemin, *Le formalisme contractuel. Mécanisme de protection de la partie faible,* Brussels, Larcier, 2010. See also the Case Law of the European Court of Justice: "the system of protection introduced by the Directive is based on the idea that the consumer is in a weak position vis-à-vis the seller or supplier, as regards both his bargaining power and his level of knowledge. This leads to the consumer agreeing to terms drawn up in advance by the seller or supplier without being able to influence the content of those terms" (E.C.J., 26 October 2006, C-168/05, *Mostaza Claro,* ECLI:EU:C:2006:675, point 25; see also E.C.J., 27 June 2000, aff. C-240/98 à C-244-98, *Oceano Grupo,* point 25; E.C.J., 4 June 2009, aff. C-243/08, *Pannon GSM Zrt*, point 22; E.C.J., 6 October 2009, aff. C-40/08, *Asturcom Telecommunicaciones SL,* points 29-31; E.C.J., 9 November 2010, aff. C-137/08, *VB Pénzügyi Lizing Zrt.,* points 46-48; E.C.J., 15 March 2012, aff. C-453/10, *Pereničová et Perenič*; E.C.J., 3 October 2013, aff. C-59/12, *BKK Mobil,* point 35 or E.C.J., 3 September 2015, aff. C-110/14, *Horațiu Ovidiu Costea*, point 18).

to a professional) because they cannot negotiate the contract nor impose their own terms. In these circumstances, the professional party to the contract can take advantage of the consumer's weak position to impose unfair contract terms (unbalanced liability exemptions for instance) or use unfair commercial practices (misleading acts or omissions and/or aggressive commercial practices). Accordingly, directives were adopted to regulate and prohibit these practices (directives 93/13/EEC and 2005/29/EC) but their efficiency could be discussed.

21 The majority of aforementioned directives, as well as the Proposal, *only* apply to B2C relationships.[31] Nevertheless, in some cases, contract relationships could be established between consumers (C2C). Most EU protection rules are not applicable in that case. The general contract law, however remains applicable in each Member State (information requirements, good faith, consent, rules of proof, etc.)[32] Nevertheless, in most cases these rules do not take into account the specific difficulties of the contracting parties. In the meaning of such rules, the parties are indeed supposed to be on an equal playing field, although it is far from the case in practice (in most cases, the rules are therefore not sufficient to protect consumers).

22 Some parties to the contract could also suffer from additional difficulties, compared with the average consumer. These may result from their age, mental or physical disability. Many children under the age of 18 (sometimes much younger) are connected to the internet, in blogs, social networks or apps. They are recipients of all kinds of publicity and contracts could be concluded by minors (to play games on a mobile device for instance). We can only regret that very few rules within the European legal framework take into account this specific problem.[33] Regarding legal minors specific (lack of experience, uninformed consent, and possible abuses by the other party), more explicit rules should be adopted.[34]

C. Articulation with concepts used under the EU horizontal framework protecting consumers

23 The concepts used in the directives protecting consumers shall be taken into account when determining whether these regulations are applicable or not. In the provisions dedicated to the scope "*ratione materiae*" of the regulations, reference is made to the concepts of "products", "goods", "services", "sales contracts", or "service contracts". It is therefore important to establish how far the "digital content" or the "contract with the object of digital content" shall also be included in such concepts of not. It is important in order to assess the global consistency of the concepts used within the EU legal framework to protect consumers. At the same time, it could also highlight some potential issues resulting from the application of various regulations. This issue shall not be exaggerated, as it is already addressed by Article 4 (7) of the Proposal: "if any provision of this Directive conflicts with a provision of another Union act governing a specific sector or subject matter, the provision of that other Union act shall take precedence over this Directive".

I. Digital content and the concepts of "product", "goods" and "service"

24 In the Unfair Commercial Practice Directive, the broad concept of "product" is used: it means "any goods or service including immovable property, rights and obligations".[35] Digital content under the Consumer Rights Directive or under the Proposal

31 Directive 2000/31/EC on electronic commerce has a broader scope. It applies to B2B (when the service provider and the recipient of the service are not acting for purposes which are outside their trade, business or profession) and to B2C relationship (when the service provider is acting in the course of his trade, business or profession and the recipient of the service is an individual consumer). The definition of "service provider" does not prohibit a consumer from providing an information society service; for instance, any natural person could sell on their blog some goods found in their attic, for private purposes. In any case, taking into account the concept of "service" and the duties required by Articles 10 and 11 of the directive, it may be argued that the European legislator has not considered that the service provider could be a consumer. Indeed, it appears out of proportion to require that the seller (in this example) must provide the recipient of the service, information on the "different technical steps to follow to conclude the contract" (art. 10, § 1, a), "acknowledge the receipt of the recipient's order without undue delay and by electronic means" (art. 11, § 1) or "makes available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order" (art. 11, § 2). Hence, those articles of the directive on electronic commerce only apply in B2C and B2B relationships.

32 On the application of general contract law to C2C relationships on online auction websites, Ch. Riefa, "La protection des consommateurs sur les plates-formes de courtage en ligne: point de vue d'outre-manche", *Revue européenne de droit de la consommation – European Consumer Law Journal*, 2005/4, p. 336-340.

33 See Art. 5 (3) and point 28 of Annexe I of directive 2005/29/EC on unfair commercial practices.

34 On the protection of minors, see M. Demoulin, «Les mineurs et le commerce électronique: besoin de protection ou d'autonomie?», *Journal des Tribunaux*, 2007, p. 105 et *seq.*; A. Nottet, «Mineurs et téléphonie mobile», *Revue Générale de Droit Civil*, 2008, p. 239 *et seq.*

35 Art. 2 (c) of the Unfair Commercial Practices Directive.

shall normally be considered as a "product" (whether falling under the meaning of "service" or under the meaning of "rights and obligations"). It means that this directive, prohibiting misleading and aggressive business-to-consumer commercial practices shall be observed when such practices are related to digital content.

25 For the purpose of the directive 1999/44/EC on sales of consumer goods, "consumer goods" shall mean "any tangible moveable item [...]".[36] Accordingly, immovable or intangible items are not covered by the directive. With reference to our study, it is necessary to determine whether digital contents can be considered as tangible or not. No definition of "tangible item" is provided in the legal provisions. Discussion usually focused on software's inclusion in (or exclusion from) the scope of the directive. Among legal scholars, there is no unanimously accepted solution. In the opinion of some, it is a tangible item,[37] while others make a distinction between the software executed at a distance (for instance, through the internet), which would be intangible and the software recorded on a physical medium (hard disk, CD-ROM, etc.), which would be tangible.[38]

26 The concepts of "goods" and "services" are used in the Consumer Rights Directive. "Goods" means "any tangible movable item".[39] "Services" are not defined by the directive but they should normally have the meaning provided by Article 57 of the Treaty on the Functioning of the European Union. Pursuant to Recital 19 of the directive, "if digital content is supplied on a tangible medium, such as a CD or a DVD, it should be considered as goods within the meaning of this directive". What about the digital content not supplied on a tangible medium (for instance supplied online through streaming)? Unfortunately, no answer is given by the Recitals (or the articles) of the directive. Regarding the residual character of the concept of "service", it is reasonable to opine that the digital content not supplied on a tangible medium should be considered as a service.

27 As a result, following the interpretation made to the provisions of the Consumer Rights Directive and the directive 1999/44/EC on the sales of consumer goods, digital contents supplied on a tangible medium are goods (and fall within the scope of the corresponding provision applicable to goods in both directives), while digital contents not supplied on a tangible medium are services (and only fall within the scope of the Consumer Rights Directive, in the provisions applicable to the services).[40]

II. Digital content and the concepts of "sales contract" and "service contract"

28 Under the Consumer Rights Directive, "sales contracts" means "any contract under which the trader transfers or undertakes to transfer the ownership of goods to the consumer and the consumer pays or undertakes to pay the price thereof, including any contract having as its object both goods and services",[41] and "service contracts" means "any contract other than a sales contract under which the trader supplies or undertakes to supply a service to the consumer and the consumer pays or undertakes to pay the price thereof".[42] It must be stressed that in both definitions, the payment of a price is a *sine qua non* condition, in order to qualify the contract accordingly. Following the Recital 19 of the Consumer Rights Directive, "similarly to contracts for the supply of water, gas or electricity, where they are not put for sale in a limited volume or a set quantity, or of district heating, contracts for digital content which is not supplied on a tangible medium should be classified, for the purpose of this directive, neither as sales contracts nor as service contracts".

29 As summarised in the DG Justice Guidance Document, a distinction is made, under the directive, between four kinds of contracts: (1) sales contracts; (2) service contracts; (3) contracts for the supply of digital content which is not supplied on a tangible medium; and (4) contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume of set quantity or of district hearing.[43]

36 Art. 1 (2)(a) of the directive.

37 M. Tenreiro and S. Gómez, "La directive 1999/44/CE sur certains aspects de la vente et des garanties de biens de consommation", *Revue européenne de droit de la consommation,* 2000, p. 12.

38 L. Serrano, «Article 1er. Champ d'application et définitions», M.C. Bianca, S. Grundmann and S. Stijns (dir.), *La directive communautaire sur la vente - Commentaire,* Brussels, Bruylant, Paris, L.G.D.J., 2004, p. 130. See also Ch. Biquet-Mathieu, «La garantie des biens de consommation – Présentation générale», *La nouvelle garantie des biens de consommation et son environnement légal*, Brussels, La Charte, 2005, p. 64-65 (who considered that software or audio/video recordings «sold» on a physical medium are tangible items and admitted that the question was controversial as concerns downloading).

39 Art. 2 (3) of the Consumer Rights Directive ("with the exception of items sold by way of execution or otherwise by authority of law ; water, gas and electricity shall be considered as goods within the meaning of this Directive where they are put up for sale in a limited volume or a set quantity".

40 See below for a discussion on this point.

41 Art. 2 (5) of the Consumer Rights Directive.

42 Art. 2 (6) of the Consumer Rights Directive.

43 DG Justice Guidance Document, op. cit., p. 5.

30 Accordingly, some provisions of the directive refer to the "contracts for the supply of digital content which is not supplied on a tangible medium". They deal with: consumer information for contracts other than distance or off-premises contracts;[44] information requirements for distance and off-premises contracts;[45] the starting point of the right of withdrawal period;[46] the penalty in the case of supply of digital content in breach of information duties;[47] and the exception, under conditions, from the right of withdrawal.[48] Article 17 of the directive also stipulates that Articles 18 (on delivery) and 20 (on passing of risks) shall not apply to such contracts, while Articles 19 (on fees for the use of a means of payment), 21 (on communication by telephone) and 22 (on additional payment) apply to them.

31 No reference is made to the "contracts for the supply of digital content which *is* supplied on a tangible medium". As the digital content supplied on a tangible medium is considered as a good, it is probably considered by the European Legislator that the contract for the supply of such item is a "sales contracts", in the meaning of the Consumer Rights Directive (governed by the corresponding provisions).

32 It must be pointed out that under Belgian Law, the distinction between these four kinds of agreements was not implemented in the legal framework, more precisely in Books VI and XIV of the Code of Economic Law (where the Consumer Rights Directive is transposed). The Belgian legislator is indeed of the opinion that the "supply of digital content which *is not* supplied on a tangible medium" shall be considered as "service contracts".[49] Accordingly, when determining the starting point of the right of withdrawal's period, no reference is made to this kind of agreement (this is however not really an issue, seen as the starting point – the conclusion of the agreement – is similar, in the directive, for both kinds of agreements).[50] The concept is however used in the list of exceptions from the right of withdrawal.[51]

33 It could be considered that the Belgian legislator has breached its duties of transposition of the Consumer Rights Directive, being agreed that it is a maximal harmonisation directive.[52] Although the protection rules prescribed by the directive shall also be applicable to the digital contents considered as services, the main differences lie in the exclusion of some digital contents from such protection rules (contrary to the directive). Indeed, the concept of "digital content" shall also apply to data or services where the counter-performance is not the payment of a price in money. However, the contract on such data cannot be considered as a service contract since the payment of a price is a requirement to qualify it as such (see above, the definition of "service contracts" under the Consumer Rights Directive). It means for instance that, when the consumer has downloaded free apps on his mobile phone, they cannot benefit from the protection rules applicable to distance contracts under the Belgian legal framework, while it should normally benefit from them under the Consumer Rights Directive.

III. Weakness of the current legal framework – corrected under the Proposal?

1. Current legal framework

34 As understood under the current legal framework at the EU level (and even more at the Belgian level for instance), the concept of digital content on one hand, and the other concepts used in the horizontal framework protecting the consumer on the other hand, raise some issues. First of all, the legal framework is very complex since various concepts must be articulated together: products, digital contents, goods, services, digital content supplied on a tangible medium, digital content not supplied on a tangible medium, sales contract, service contract, and (contract on the) supply of digital content not supplied on a tangible medium. In addition, the concepts are structured on the Russian Doll Model: the digital content is a sort of "goods" or "services", themselves considered as a sort of "products"; the contracts on the supply of digital contents are sort of "sales contracts"; and contracts for the supply of digital content not supplied on a tangible medium constitute an autonomous category of contracts or, under Belgian Law, are qualified as service contracts. Although it is not an insular solution in Law, it means that lawyers shall make a distributive application of the protection measures. First, they shall apply the specific rules dedicated to the digital content

44 Art. 5 (2) of the Consumer Rights Directive.

45 Art. 6 (2) of the Consumer Rights Directive.

46 Art. 9 (2) (c) of the Consumer Rights Directive.

47 This is the case when "(i) the consumer has not given his prior express consent to the beginning of the performance before the end of the 14-day period referred to in Article 9; (ii) the consumer has not acknowledged that he loses his right of withdrawal when giving his consent; or he trader has failed to provide confirmation in accordance with Article 7(2) or Article 8(7)" (Art. 14 (4) (b) of the Consumer Rights Directive).

48 Art. 16 (m) of the Consumer Rights Directive.

49 *Doc. Parl.*, Ch. Repr., sess. ord. 2012-2013, n° 3018/001, p. 16.

50 Art. VI.47 of the Belgian Code of Economic Law.

51 Art. VI.53, 13, of the Belgian Code of Economic Law.

52 Art. 4 of the Consumer Rights Directive.

and then, depending on the digital content at stake, the general rules on goods, services, sales contract or service contract. In the provisions related to the right of withdrawal, it should be easier with a set of rules applicable to digital contents, next to another set of rules applicable to services and goods. In addition, a distinction is made whether the digital contents is supplied on a tangible medium or not.[53]

35 In the first case, it is considered as a goods (subject to a sales contract), with the correlative application of the protection measures prescribed by the directive 1999/44/EC on the sales of consumer goods and the specific rules regarding the right of withdrawal (with determined starting point and exception from the right of withdrawal). As soon as this digital content is subject to a sales contract (requiring payment), it means that the digital contents provided for free – i.e. without any payment – are excluded from the protection measures related to the right of withdrawal. This issue should however remain theoretical; namely, when no payment was made, the consumer can terminate the agreement easily without penalty or risk of non-reimbursement. In the other case, it is considered as a service (subject to a contract for the supply of digital content not supplied on a tangible medium), out of the scope of the directive 1999/44/EC on the sales of consumer goods and with other rules regarding the right of withdrawal. It means nevertheless that digital contents shall benefit, in that case, from the protection measures related to the right of withdrawal.

36 Such discrimination is not justified at all. Even less so since the content as such is equivalent in both cases – i.e the same software or film, regardless of whether it is downloaded online or supplied on a CD-ROM delivered by traditional mail. Furthermore, when considering that the digital content supplied on a tangible medium is a good subject to a sales contract, a confusion arises between the medium, protected by classical property rights (real right implying *usus*, *fructus* and *abusus*), and the content, usually protected by copyrights and on which the consumer does not have similar rights (only a limited right to use).

37 The current situation is summarised in the table below:

		Goods	Sales contract	Service	Service contract	Contract for the supply of digital content not supplied on a tangible medium
CRD	Digital content supplied on a tangible medium	YES	YES	NO	NO	NO
	Digital content not supplied on a tangible medium	NO	NO	YES	NO (except under Belgian Law)	YES

2. Strengths of the Proposal and remaining issues

38 Hopefully various issues of the current legal framework, as described above (see point C.III.1.) are addressed in the Proposal. There is no discrimination regarding whether digital content was supplied on a tangible medium or not – both shall benefit from equivalent protection measures, regarding conformity requirements or termination of the agreement. The legal framework is therefore consistent for all kinds of digital contents. Furthermore, it is clearly stated that the legal framework shall apply no matter the counter-performance as the supply of the digital content is the payment of a price or the processing of personal data or other data. The legal framework remains very complex because no modification is made to the Consumer Rights Directive. This directive should however be amended in order to include the new definition of "digital content" prescribed by the Proposal.

39 Discussions could also arise with regard to the digital content embedded in goods (which should occur frequently in the near future, with the development of artificial intelligence and automatisation). In case of defect, which set of rules is applicable? The rules applicable to goods or the rules applicable to digital contents (should the proposal be adopted)? This point is currently under discussion before the Council,[54] where three options were proposed: (i) application of "goods rules" to the embedded digital content; (ii) split approach with respective application of "goods rules" to goods and application of the Proposal to the embedded digital content; and

53 For an analysis of this topic (the distinction between physical medium or other provision means, and the content – data base, software, etc. –, as well as the qualification of each element), see S. Dusollier, *Droit d'auteur et protection des œuvres dans l'univers numérique,* Brussels, Larcier, 2007, p. 398 *et seq.*; E. Montero, *La responsabilité civile du fait des bases de données,* Namur, PUN, 1998, p. 238 *et seq.*; A. Lucas, "La responsabilité civile du fait des 'choses immatérielles'", *Etudes offertes à Pierre Catala – Le droit privé français à la fin du XX^e siècle,* Paris, Litec, 2001, p. 816 *et seq.*

54 Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content (First reading) - Policy debate, ST 14827 2016 INIT - 2015/0287 (OLP).

(iii) application of the Proposal to both goods and embedded digital content, "with an exception giving the supplier the possibility to prove that the defect lies in the hardware of the good, in which case the 'goods rule' would be applied when remedying such a defect". From a strictly legal point of view, option ii) is the most accurate. It could however engender difficulties when determining whether the defect is related to the digital content or to the goods where it is embedded. Option iii) should in this context ensure a higher level of protection to the benefit of the consumers, being agreed that whenever possible, the rules applicable to goods and to digital contents should be equivalent.

D. Articulation with other relevant concepts under (classical) Civil Law

40 Rules related to the general theory of contract law are prescribed by the French Civil Code of 1804[55] – also called the Napoleon Code – as well as by the Belgian Civil Code.[56] They deal, among others, with the requirements to the validity of the contract, the effect of the contract (between the parties and towards third parties), and with the sanctions, should there be a breach by a party of its contractual duties. Only few modifications have been brought to these provisions since 1804 and both legal frameworks (French and Belgian) remained similar (although distinctions resulting from the respective case law of both countries could not be excluded). Amendments were made recently in France with the adoption of a new set of legal provisions that came into force on 1st October 2016.[57]

41 In both Civil Codes, some provisions mostly unchanged since 1804, are also applicable to the so-called named agreements ("contrats nommés"), i.e. the agreements which for a specific legal framework is provided by the Code. Regarding the aim of the present paper, we will only focus on the sales contract[58] ("vente") and on the contract of enterprise[59] ("louage d'ouvrage et d'industrie"). It must be stressed that most rules were drafted, in 1804 considering the usual object of such agreements at that time – the sale or the construction of buildings and other immovable goods. Regarding the sales contract, the legal framework is somewhat elaborate, with provisions on the requirements of the sales (who is allowed to buy or to sell? What can be sold?), the duties of the seller (conform delivery,[60] warranty for hidden defects,[61] and warranty for quiet possession[62]) the duties of the buyer (mainly paying the price) and the termination of the agreement. The chapter on the "contract of enterprise" is very poor, with only few provisions (mostly out-dated). Attention must nevertheless be paid to the Case Law, that has provided some useful interpretation of the rules, and has applied them in other contexts (notably in the context of IT Contracts and Information and Communication Technologies).

42 These rules related to the general theory of contract law and the named agreements of the Civil Code shall only be applicable provided that a specific legal provision does not further exist (should there be any inconsistency between the general rule of the Civil Code and a specific rule prescribed by an Act, the specific rule shall prevail). Furthermore, most of these rules are not mandatory and the parties are therefore allowed to derogate to them by contract (which is usually the case). Essentially, they can be seen as a toolkit used by the Parties when elaborating their *sui generis* agreements.

43 The qualification of "software" is a good example (it can indeed be considered as digital content). Discussions usually arise when deciding whether the contract on such software must be considered as a sales contract or as another kind of contract (for instance, a contract of enterprise or *a sui generis* contract).[63] A distinction is usually made between "standard software" and "custom software", designed upon request of the client. The contract on custom software, where a right to use – a license – is granted to the client, is usually qualified under Belgian and French Law as a contract of enterprise (being agreed that, regarding the tangible medium used to supply the software, the contract is considered as a sales contract). Regarding the "standard software", there is not any consensus among legal scholars and there is not any clear judgement stating in a sense or in the other. Some authors consider that it is indeed somewhat disputable to refer to a "sales contract" when – except for the tangible medium used to supply it – the client is only granted a right to use the

55 See Art. 1100 *et seq.* of the French Civil Code.

56 See Art. 1101 *et seq.* of the Belgian Civil Code.

57 Ordonnance n° 2016-131 of 10 February 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.

58 Art. 1582 *et seq.* of both Civil Codes.

59 Art. 1779 et seq. of both Civil Codes.

60 «Obligation de délivrance conforme».

61 «Garantie des vices cachés».

62 «Garantie d'éviction».

63 On this topic, see E. Montero, *Les contrats de l'informatique et de l'internet*, Brussels, Larcier, 2005, p. 72 *et seq.* ; J. Huet, "De la 'vente' de logiciel", *Etudes offertes à Pierre Catala – Le droit privé français à la fin du XXe siècle*, Paris, Litec, 2001, p. 799 *et seq.*; M. Vivant *et al.*, *Lamy Droit du Numérique*, Paris, Kluwer, 2016, n. 719 *et seq.* ; A. Lucas, J. Deveze et J. Frayssinet, *Droit de l'informatique et de l'internet*, Paris, P.U.F., 2001, p. 488 *et seq.*; Ph. Le Tourneau, *Contrats informatiques et électroniques*, 7e éd., Paris, Dalloz, 2012, p. 203 et seq.

software (a license). This right to use is governed by copyright law, which is different from the classical property law applicable to tangible items. On the other hand, the "standard software" already existed before the conclusion of the agreement; as a result, the IT provider did not carry out any task in order to elaborate the software (as it should normally be the case in a contract of enterprise).

44 As far as most rules applicable to sales contracts and to the contract of enterprise are not mandatory, parties remain free to determine their respective rights and duties (and they usually do so with some reference to rights and duties prescribed to the sales contract and to the contract of enterprise). Under French and Belgian Law, the freedom of contract is indeed a key principle. In this context, and being agreed that neither the qualification of sales contract, neither the qualification of contract of enterprise is 100% satisfactory, the most appropriate qualification is probably a "*sui generis* agreement", where the parties freely decide the rights and duties of each other.

45 A Judgement rendered by the Court of Appeal in Luxembourg is, in this context, very interesting.[64] The dispute was about the breach in the delivery of a standard software. The operation was qualified "sales" by the Parties and the Court consecrated such qualification, with this important comment: the buyer of such an item will not have the same rights and duties than a buyer of any movable tangible item (subject to a right of property); in the case of the standard software, a right to use will be granted to the client, subject to copyright Law. In fact, the sole practical interest of a qualification process is the application of the material protection rules associated to such qualification. On this point, the Court added that the rights and duties of the parties are roughly the same,[65] no matter the qualification (sales, contract of enterprise, etc.).[66]

46 With the Proposal, the consumer receiving a software, whether standard or custom, shall benefit from the protection measures (conformity, termination, etc.) and the remedies established by the directive (should it be adopted). The discussion on the qualification as a sales contract or as a contract of enterprise will become useless. In that sense, the Proposal will contribute to the simplification of the legal framework, and with a higher level of protection to the benefit of the consumers. Between professionals, however, the contract law rules prescribed at the national level shall remain applicable. Incidentally, under French Law, it is highly probable that the implementation of the Proposal will be made in the Code of Consumer Law. New provisions of the sale of consumer goods were indeed included in this Code of Consumer Law (Art. L217-1 *et seq.*), which is consistent regarding the scope of the provisions (B2C).

47 Contrariwise, in order to implement the directive 1999/44/EC on sales of consumer goods into national Law, the Belgian legislator has introduced the new legal provisions in the Civil Code, in the chapter consecrated to the sales contract (Art. 1649*bis et seq.* of the Belgian Civil Code). Other legal provisions protecting consumers – prohibition of unfair commercial terms or unfair commercial practices, for instance – are included in the Code of Economic Law and it would sound logical that the Proposal shall be implemented into this Code. An even better option could be the elaboration of a Code of Consumer Law under Belgian Law, where all these rules protecting consumers could be brought together, including the provisions implementing the directive 1999/44/EC on sales of consumer goods.

E. Conclusion

48 Digital contents are currently defined and regulated by the Consumer Rights Directive (information duties and specific provisions on the right of withdrawal). Various issues arise out of the articulation between the concept of "digital content" and other relevant concepts of the Consumer Rights Directive, such as "goods", "services", "sales contract", and "service contracts". Digital contents supplied on a tangible medium shall indeed be considered as goods (and the contract on such content as "sales contract"), when digital contents not supplied on a tangible medium shall be considered as "services" (and the contract on such content as a "contract for the supply of a digital content not supplied on a tangible medium"). Such differences are a source of futile complexity, and they could give rise to unjustified discrimination.

49 The Proposal offers satisfactory answers to many of the issues resulting from the conceptual legal framework applicable to the digital contents (there is no distinction whether it is supplied on a tangible medium or not, application to digital contents supplied with personal data or other data as counter-performance, etc.), although some difficulties will remain.

50 Regarding the articulation with the classical concepts

64 C.S.J. Luxembourg, 5 February 2003, *DAOR*, 2003/67, p. 47, note H. Jacquemin.

65 Some differences could however be highlighted.

66 The Court states that «*les obligations des parties (obligation de délivrance, de garantie des vices, de conseil et d'information du côté du fournisseur, et obligation de collaborer et de payer le prix convenu du côté de l'utilisateur) sont essentiellement les mêmes que le contrat soit qualifié de vente, de bail (acquisition d'une licence) ou encore de contrat de vente complétée par un contrat d'entreprise*».

of "sales contract" or "contract of enterprise", we do not expect major issues. Most of these rules are not mandatory and, when a claim is brought before the courts in order to discuss the qualification of a digital content (a software) under these categories, there is not any unanimity among legal scholars and within case law. The existence of a specific legal framework protecting consumers should simplify the analysis, as the application the Contract Law rules shall not be necessary anymore (except in B2C and C2C relationships).

51 In terms of next steps, we are of the opinion that all these provisions protecting consumers, especially in the recent proposals made by the Commission, should be included in a single legal instrument (a Code of Consumer Law, for instance), where the higher level of consistency and harmonization is ensured between the legal frameworks (without any unjustified discrimination between the conformity for goods or digital content, simplified information duties, etc.).

Interoperability in the Digital Economy

by **Wolfgang Kerber**, professor of Economics, Marburg Centre for Institutional Economics, School of Business & Economics, Philipps-University Marburg

and **Heike Schweitzer**, professor of Law and Managing Director of the Institute for German and European Economic Law, Competition Law and Regulatory Law, Freie Universität Berlin

Abstract: Interoperability has become a buzzword in European policy debates on the future of the digital economy. In its Digital Agenda, the EU Commission has identified a lack of interoperability as one of the significant obstacles to a thriving digital economy. The EU Commission and a number of other actors have advocated far-reaching policies for ensuring the interoperability of digital goods, services, platforms and communication networks. In this paper, we present a systematic framework for discussing interoperability problems from an economic and legal perspective and apply it to several interoperability issues such as, e.g., standardization, interoperability regulation in the field of electronic communication, duties of dominant firms (including platforms) to ensure horizontal and vertical interoperability and IP law exceptions in favor of interoperability. The complex trade-offs between benefits and costs of a higher degree of interoperability suggest the need for a careful and separate analysis of each specific interoperability issue, caution regarding a (top down) imposition of mandatory standards and interoperability obligations, and a greater focus on unilateral solutions of interoperability problems, such as adapters or converters. Within the framework of Art. 102 TFEU, EU competition law may be better advised to develop a workable test to address hurdles for unilateral interoperability solutions created by dominant firms, than to continue focusing on the essential facilities doctrine to mandate interoperability.

Keywords: Interoperability; standards; digital economy; digital goods; platforms; communication networks

Recommended citation: Wolfgang Kerber and Heike Schweitzer, Interoperability in the Digital Economy, 8 (2017) JIPITEC 39 para 1.

A. Introduction

1 Interoperability has become a buzzword in European policy debates on the future of the digital economy. In its Digital Agenda, the EU Commission has identified a lack of interoperability as one out of seven[1] "most significant obstacles" to the "virtuous cycle" of digitalization.[2] Effective interoperability between networks, devices, applications, data repositories and services has thus become a major goal of the European Digital Agenda, which aims to stimulate the emergence of "a truly digital society" and to boost innovation and European competitiveness.[3] Significant market players shall be led to pursue interoperability-friendly business policies.[4]

1 The other obstacles are: fragmented digital markets; rising cybercrime and risk of low trust in networks; lack of investment in networks; insufficient research and innovation efforts; lack of digital literacy and skills; and missed opportunities in addressing societal challenges – see EU Commission, A Digital Agenda for Europe, Brussels, 19.5.2010, COM(2015)245 fin., p. 5-6.

2 EU Commission, A Digital Agenda for Europe, Brussels, 19.5.2010, COM(2010)245 fin., p. 3.

3 See, for example, EU Commission, A Digital Agenda for Europe, Brussels, 19.5.2010, COM(2010)245 fin., p. 14-15; EU Commission, A Digital Single Market Strategy for Europe, Brussels, 6.5.2015, COM(2015)192 fin.

4 See EU Commission, A Digital Agenda for Europe, Brussels, 19.5.2010, COM(2010)245 fin., p. 15: The Commission will examine the feasibility of measures that could lead significant market players to license interoperability information while at the same time promoting innovation and competition".

2 Indeed, in an interconnected economy, interoperability of a broad variety of networks, devices and services will be key.[5] The expected benefits of the Internet of Things and Industry 4.0 hinge on the interoperability between networks, software and data. Yet, interoperability is a complex concept. Any interoperability policy which strives to intervene into the market-driven determination of the degree of interoperability will come at a cost. Such trade-offs must be taken into account.

3 In our paper, we shall offer a systematic framework for discussing interoperability and the EU's interoperability policy, and we will analyze the existing legal framework on this basis. In chapter B., we introduce the concept of interoperability, provide an overview of its benefits and costs and the ensuing tradeoffs, and show that the market determination of interoperability can be subject to serious market failures where the degree of interoperability is determined unilaterally by a dominant firm, or where the market gravitates towards a uniform technical standard with natural monopoly characteristics. In the following chapters (C.-F.), we shall inquire how these insights translate into law and public policy. Both law and public policy have to consider that the need for interoperability may differ depending on the market setting, and that different paths towards interoperability exist, all of which have both advantages and costs. In certain settings public intervention may be justified; however, there should be a clear and strong reason for mandating and/or regulating interoperability.

4 Firstly, we shall look at standard-setting in this light, analyzing the different variants of standard setting, with a focus on the EU Commission's pro-collective standard-setting policy (C.). Electronic communications networks provide an example where mandated interoperability may be justified – based in particular on a public service rationale. This rationale cannot easily be extended to digital platforms, however (D.). Competition law should be cautious in imposing interoperability remedies, in particular when they are based on a vague and potentially over-broad "essential facilities"-doctrine (E.). Instead, law and policy should focus more on protecting market solutions to non-interoperability. On the side of IP law, both the Software Directive[6] and the Trade Secret Directive[7] provide for decompilation exceptions to promote unilateral efforts to ensure interoperability. Competition law may apply where dominant firms try to hamper competitors in their efforts to invent around interoperability impediments. Taken together, these two instruments may be a promising and innovation-friendly alternative to broad public interoperability mandates (F). Chapter G. will conclude.

B. Interoperability: Benefits, costs, trade-offs, and market failure

I. What is interoperability?

5 One of the difficulties of the interoperability discussion is the absence of a clear definition of interoperability. Broadly speaking, interoperability denotes the ability of a system, product or service to communicate and function with other (technically different) systems, products or services. Interoperability issues in the digital economy will typically relate to information exchange and data. In this context, Palfrey and Gasser, two leading figures of the interoperability debate, define interoperability as the "ability to transfer and render useful data and other information across systems, applications, or components".[8] The EU Software Copyright Directive[9] and the EU Draft Directive on Digital Goods and Services[10] entail similar, but more context-specific definitions. Interoperability is thereby a sub-category of the broader, but also vaguer concept of compatibility; namely the "ability of two or more systems or components to perform their required functions while sharing the same hardware or software environment".[11] Since it is the communication and exchange between systems, products and services that is key in the digital economy, we shall focus on the concept of "interoperability".[12] The boundaries

5 For a broad account of the role of interoperability in the digital environment see Palfrey/Gasser, Interop, 2012.

6 Directive 2009/24/EC on the legal protection of computer programs.

7 Trade Secret Directive 2016/943 of 8 June 2016, OJ 2016 L 157/1.

8 Palfrey/Gasser, Interop, 2012, p.5, and the „Standard Glossary of Software Engineering Terminology" (IEEE 610) of the Institute of Electrical and Electronics Engineers: Interoperability is „[t]he ability of two or more systems or components to exchange information and to use the information that has been exchanged ...".

9 Directive 2009/24/EC on the legal protection of computer programs. See recital 10: "The function of a computer program is to communicate and work together with other components of a computer system and with users and, for this purpose, a logical and, where appropriate, physical interconnection and interaction is required to permit all elements of software and hardware to work with other software and hardware and with users in all the ways in which they are intended to function."

10 According to Art. 2 No. 9 "interoperability means the ability of digital content to perform all its functionalities in interaction with a concrete digital environment".

11 See the „Standard Glossary of Software Engineering Terminology" (IEEE 610) des Institute of Electrical and Electronics Engineers.

12 In this context the relation between the concepts of

that systems share and allow them to connect and exchange information are called "interfaces".[13] Often interoperability will be based on the access to a (technical) standard.[14]

6 Interoperability can be relevant on different layers; for example, syntactic/technical interoperability refers to the possibility that systems can physically connect to each other and can exchange data, whereas semantic interoperability refers to the ability of systems to understand the meaning of the information exchanged.[15] Particularly important is the distinction between horizontal and vertical interoperability. Horizontal interoperability denotes the interoperability of competing products, services or platforms. One example is the interconnection between communication networks.[16] Vertical interoperability refers to the interoperability of a product, service or platform with complementary products and services. The degree to which complementary products (e.g., digital goods as music files or e-books) can be shared across different platforms, and complementary products of one platform can be accessed from rival platforms is said to characterize the horizontal openness of a platform. The ability of independent firms to offer complementary products on a platform stands for its vertical openness.[17] Both horizontal and vertical interoperability can be a matter of degree. First, technically there can be a continuum between full and no interoperability (with different degrees of partial interoperability, as, e.g., in regard to the number of functionalities). For example, interoperability issues may arise between different versions of software (upward and/or downward compatibility). Secondly, achieving interoperability may come at a cost, e.g. the monetary cost of developing adapters and converters, and the inconvenience of applying them. Thirdly, interoperability and openness can be symmetric or asymmetric, e.g., the products of platform A can be used on platform B, but not vice versa. There is, in other words, a wide continuum between no and full interoperability, with many different intermediate designs of partial interoperability between both extremes.

7 The extent and specific design of the interoperability of products, services, and platforms of a firm is influenced by both technological decisions and legal constructs.[18] Namely, it depends not only on (1) technological decisions of the firm but also on (2) its decisions (a) to allow interoperability through contractual arrangements with customers and suppliers, (b) its willingness to disclose the necessary interface information and (c) its toleration of the unilateral development of adapters and converters by other firms. The different forms and degrees of interoperability indicate the complexity of the interoperability issue.

II. Benefits and Costs of Interoperability: An Overview

8 Even among the proponents of greater interoperability, there is a broad consensus that (1) interoperability is not an aim in itself, (2) there are both benefits and costs of interoperability, and (3) due to the ensuing trade-offs, the optimal degree and design of interoperability will be context-specific and will depend on the specific economic and technological conditions in a market.[19] The following overview shall explain the potential benefits and costs of interoperability in a general way before we

compatibility and interoperability are often not clear, which also explains the inconsistent use in the literature.

13 See the "Standard Glossary of Software Engineering Terminology" (IEEE 610) des Institute of Electrical and Electronics Engineers, and Directive 2009/24/EC, recital 10: "The parts of the program which provide for such [see Footnote 2] interconnection and interaction between elements of software and hardware are generally known as 'interfaces'."

14 A (technical) standard is a technical norm that is (or shall be) broadly used in the marketplace in order to ensure compatibility or interoperability – see OECD, Data-Driven Innovation. Big Data for Growth and Well-Being, 2015, pp. 110.

15 With their suggestion of four different layers of interoperability (technological, data, human, institutional) Palfrey/Gasser, Interop, 2012, p. 6, 39-53) emphasize that interoperability should not only be seen as a primarily technical problem but should also encompass the level of humans and institutions.

16 "Interconnection" means the physical and logical linking of public communication networks used by the same or a different undertaking in order to allow the users of one undertaking to communicate with users of the same or another undertaking, or to access services provided by another undertaking – see Art. 2 lit. (b) of the Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communication networks and associated facilities, OJ 2002 No. L 108/7 ("Access Directive").

17 Farrell/Simcoe, Four Paths to Compatibility, in: Peitz/Waldfogel, The Oxford Handbook of the Digital Economy, 2012, 34, 36-37. Since in the digital economy complex interconnected value networks have emerged, the distinction between horizontal and vertical interoperability might not always be so clear anymore.

18 From a business strategy perspective, see also Shapiro/Varian, Information rules, 1999, pp.193.

19 See for overviews on benefits and costs of interoperability Choi/Whinston, Benefits and requirements for interoperability in the electronic marketplace, Technology in Society 22, p. 33; Gasser, Interoperability in the Digital Ecosystem, 2015, pp. 9-17; available at SSRN: <http://ssrn.com/abstract=2639210>; Farrell/Simcoe, Four Paths to Compatibility, in: Peitz/Waldfogel, The Oxford Handbook of the Digital Economy, 2012, 34, 36-38; more specifically with regard to standards LaRouche/Overwalle, Interoperability standards, patents and competition policy, TILEC Discussion paper, 2014, pp.15-18.

come to assess the Commission's interoperability policy within the context of the existing legal framework.

9 Uniform standards allow for more mass production and a lower number of product variants. The resulting economies of scale and scope as well as network externalities can bring large cost advantages. Interoperability may also allow for a modularization of components of products, which can be used for different (often customized) products. It can reduce the costs for consumers (and increase their benefits), if they can more easily combine products from different firms and share them with other consumers on different devices or platforms. Moreover, it can reduce transaction costs through lower information costs about interoperability problems. Interoperability, especially through open standards and open platforms, can boost innovation with regard to complementary products and services – an effect that may be particularly important in the digital economy. Simultaneously, interoperability increases competition with regard to these complementary products and services, which may benefit consumers through lower prices. In addition, interoperability is a precondition for the interconnectedness and free flow of data that is crucial for a data-based economy, and therefore for data-driven innovation. Further advantages of more interoperability include greater choice for consumers, easier access to products and services, and more flexibility both for firms and consumers, due to a lower degree of lock-in (both for consumers and firms).[20]

10 However, more interoperability and the use of uniform standards may also increase costs and risks both for firms and consumers. Most importantly, it can lead to a greater degree of homogeneity. To the extent that uniform standards and interfaces are used, the possibilities of firms to develop their own specific products and services are limited, because they have to comply with these standards and interoperability requirements. This will limit the scope for innovation and therefore the extent to which specific consumer preferences can be fulfilled by way of product differentiation.[21] Although greater interoperability may lead to more innovation and competition with regard to complementary products, it also can lead to less innovation and competition with regard to the standards and interfaces themselves, which may have the characteristics of natural monopolies (with all their negative consequences). Furthermore, the openness of products and platforms for complementary products can lead to higher risks for consumers, if the complementary products offered by other firms are not monitored closely with a view to their interoperability, quality, and safety. Through a generally higher level of interconnectedness in a digital economy, more interoperability may lead to higher risks regarding reliability, security, and privacy.[22] Considering these (potentially large) costs of interoperability, the policy objective should not be full or maximum interoperability, but rather an optimal degree of interoperability that balances benefits and costs.

III. Interoperability and competition: When should we expect market failure?

11 First and foremost, it is part of the entrepreneurial freedom of firms to decide themselves on the extent of the interoperability of their products and services. Selling products that are interoperable with other products, or offering an open platform that allows for sharing products and services with other platforms, can increase the value for customers and therefore increase profits. In the same way, the use of standardized components in a production value chain can reduce production costs and therefore allow for lower prices. However, firms may want to develop more innovative products and services that require more specific components and services, and/or think that the specific quality and features of their service can only be assured if they are capable of controlling the entire value network (including complementary products and services) according to their own specific requirements. A large degree of interoperability and openness to complementary products the quality and safety of which they cannot control may then endanger their business model. As a consequence, they may opt for a closed instead of an open system. A good example for such a business model is Apple: with the iOS operating system and the Apple App Store, it established a closed system, which allows for far-reaching control of all apps that run on the iOS operating system.

12 For a better understanding, it is useful to introduce the concept of modularity with interfaces and combine it with the distinction of competition between systems and competition within systems. In the (old) example of the automobile industry, it is the car manufacturer who decides on the entire product that consists of thousands of specific components in the value chain, which have to

20 See Gasser, Interoperability in the Digital Ecosystem, 2015, pp. 11-12 (available at SSRN: <http://ssrn.com/abstract=2639210>).

21 See also Palfrey/Gasser, Interop, 2012, pp.106.

22 See Gasser, Interoperability in the Digital Ecosystem, 2015, pp. 13-15 (available at SSRN: <http://ssrn.com/abstract=2639210>).

fit and interoperate but are produced by many independent suppliers. In a modularized system, the car manufacturer (or system leader) decides on the interfaces that the component suppliers have to use in order to ensure the smooth interoperability of all car components. Within such a modular system, suppliers can compete and innovate with regard to these modularized components (competition within system). However, only through competition among car manufacturers is the modular system with its specific interfaces itself subject to competition (competition between systems). Therefore, there are two levels of innovation: innovation within a system at the level of the components (but limited by the requirements of the interfaces); and innovation of the systems themselves (including the interfaces of such a modular system).[23]

13 On the market, firms compete with different business models and different degrees of interoperability. A number of customers may prefer products and platforms that offer a more closed system of complementary products and services (and which are therefore less interoperable with other systems), even if this may lead to the customers being locked-in to some extent. Other customers will value the flexibility and larger choice of more open systems, even if this is accompanied by higher risks in terms of reliability or safety, and perhaps less convenience. In the same way, the producers of components or complementary products (as apps) can decide whether they want to develop and produce their products according to general standards or want to be part of a closed system with all its specific rules. Each will have specific advantages and costs. Competition economists would claim that in markets with effective competition, the firms have incentives to decide on the extent and design of interoperability that corresponds to the preferences of their consumers (and their supplier and app developers). Therefore, as long as there is effective competition, serious market failures with regard to the extent of interoperability cannot be expected.[24]

14 The situation is very different if competition does not work well or is even impossible, e.g., due to natural monopoly problems. Two different groups of cases can be distinguished:

15 **Dominant firms:** This refers to situations in which a dominant firm already exists that can unilaterally decide on the interoperability of its products. The famous Microsoft case decided by the CFI in 2007[25] is an apt example. Due to its dominant position on the market for PC operating systems, Microsoft's decisions regarding the interoperability between its PC operating system and work group server operating systems were not effectively controlled by competition. Similar settings may gain importance in the digital economy because of the strong role of platform markets (search engine market, social media market etc.) with their strong positive network effects and tipping tendencies to quasi-monopolies.[26]

16 **Standards as natural monopolies:** In this second group of cases, there is no dominant firm at the beginning, but the economic advantages of a (technical) standard and therefore of interoperability are so large that competition between standards is not sustainable. Ultimately, only one single uniform (technical) standard should exist (natural monopoly). Due to the economic advantages of (monopolistic) technical standards, their collective establishment within the framework of standard-setting organizations (SSOs) has been promoted by public policy for a long time. Important examples in the digital economy are telecommunication standards or the DVD-standard, and we have seen the claims that a data-based economy (such as the Internet of Things) needs new technical standards for ensuring data communication in highly interconnected systems.[27]

17 While the two settings are different in many respects, law and policy have to address the following two problems in both scenarios:

(1) The situation of market dominance either at the beginning or at the end raises a danger of monopoly pricing and potential foreclosure and/or leverage options with regard to upstream / downstream markets and complementary products.

(2) There are serious concerns that the market may not be capable of identifying and implementing efficient technical standards in a competitive process. Fragmentation of standards, standard wars, and lock-in into inefficient or outdated standards may result.

23 For the advantages of modularized systems for innovation, see Baldwin/Clark, Design Rules. Vol. 1: The Power of Modularity, 2000, and MacKie-Mason/Netz, Manipulating interface standards as anticompetitive strategy, in: Greenstein/Stango, Standards and Public Policy, 2007, 281, who distinguish between systems and component competition.

24 However, effective competition cannot guarantee that the market always finds the optimal interoperability solutions. Especially in oligopolistic settings there might be problems due to collusive behavior.

25 CFI, Judgment of 17.9.2001, Case T-201/04 – Microsoft Corp.

26 Haucap/Heimeshoff, Google, Facebook, Amazon, eBay: Is the Internet driving competition or market monopolization?, Int Econ Econ Policy 2014, 49, 50 et seqq. Evans, suggests that tipping towards monopolies is usually prevented by the complexity of multi-platform markets: The Antitrust Economics of Multi-Sided Platform Markets, Yale Journal on Regulation, Vol. 20 (2003), 325, 350.

27 For an overview about the economics of standards, see Tassey, Standardization in Technology-Based Markets, Research Policy 29, 2000, 587, and Blind, The economics of standards, 2004.

18 In a comprehensive survey article about possible solutions to these interoperability problems through standard setting, Farrell/Simcoe have distinguished four different "paths to compatibility".[28] (1) Firms compete in the market for setting their own standard as the single uniform standard, which can lead to "standard wars". (2) A dominant firm may have the power to impose a standard on the market.[29] (3) Firms may agree on a new single standard through negotiation leading to the well-known solution of collective standard setting (with standard-setting organizations). In the following chapter C. we will discuss in more detail the problems of standard-setting and the advantages and problems of these three solutions. (4) A very interesting fourth solution to the problem of setting a uniform single standard (with natural monopoly problems), is the market search for adapters and converters capable of either converting a format into another or at least ensuring that a product can be used on another platform (in a similar way as electricity adapters and converters). Where this solution works, it may render the establishment of a single standard unnecessary, because they reduce network externalities and "lock-in" problems (through reducing switching costs and allowing more flexibility). Consequently, adapters may enable a sustainable coexistence of different standards, and even beneficial innovation competition between them. Chapter F. will discuss this alternative path towards interoperability with its problems and policy implications.

C. Interoperability through standardization

19 Economically, non-interoperability does not necessarily constitute, or result in, a market failure; and interoperability can be achieved in different ways. The EU Commission, however, consistently highlights the importance of interoperability as a core element of its Digital Single Market Strategy. Among the different strategies to achieve interoperability in the ICT sector, collective standard-setting enjoys the Commission's particular support:

> *"Standardisation has an essential role to play in increasing interoperability of new technologies within the Digital Single Market. It can help steer the development of new technologies such as 5G wireless communications, digitisation of manufacturing (Industry 4.0) and construction processes, data driven services, cloud services, cybersecurity, e-health, e-transport and mobile payments."*[30]

20 Standardisation has accompanied and shaped the evolution of the ICT industry for some time.[31] Apart from influential industry consortia,[32] standard-setting organizations (SSOs) have been crucial in developing open standards. The mandated development of the GSM standard by ETSI and its subsequent market roll-out is frequently considered a particular success of European standardization policy.[33]

21 The EU Commission's pro-collective standard-setting strategy can be a suitable solution for solving standardization problems. However, both theoretical analysis and empirical studies indicate that, when comparing the different modes of standard-setting (competition for standards, decisions by dominant firms, collective standard-setting) and routes for solving interoperability problems (including the development of adapters), collective standard-setting will not always be optimal.

22 A comparative analysis of the benefits and costs of different modes of standard-setting has to start with the following effects and problems of standard-setting, which affect the different forms of standard-setting in different ways:

23 **Dynamic / path dependency effects:** Interoperability standards are characterized by positive (direct and indirect) network effects: for each firm, the attraction of a given standard grows with the number of other firms and products using it. A "critical mass" of adoptors is needed for the standard to survive in the marketplace. Frequently, first-mover advantages will exist, i.e. long-term competitive advantages of the standard of an early firm in comparison to later entrants. Where standard-setting has not (yet) become a collective endeavor, firms will therefore strive

28 Farrell/Simcoe, Four Paths to Compatibility, in: Peitz/Waldfogel, The Oxford Handbook of the Digital Economy, 2012, 34, 38-47.

29 Farrell/Simcoe use a broader notion of a "dominant player" who can impose standards. Besides a dominant firm it can also be a large customer or even the government. See Farrell/Simcoe, Four Paths to Compatibility, in: Peitz/Waldfogel, The Oxford Handbook of the Digital Economy, 2012, 34, 40-42.

30 EU Commission, A Digital Single Market Strategy for Europe, Brussels, 6.5.2015, COM(2015)192 fin., p. 15.

31 Biddle et al., The Expanding Role and Importance of Standards in the Information and Communications Technology Industry, 52 Jurimetrics 177 et seq. (2012).

32 See Baron/Pohlmann, 9(4) Journal of Competition L&E 2013, 905 et seq.; Liu, International Standards in Flux: A Balkanized ICT Standard-setting Paradigm and its Implications for the WTO, Journal of International Economic Law 2014, 561, 568 et. seqq. For the relevance of standard setting by industry consortia see Van Eecke et al., EU Study on the Specific Policy Needs for ICT Standardization, July 2007, at 7, available at <http://ec.europa.eu/enterprise/sectors/ict/files/full_report_en.pdf>.

33 For a closer analysis: Audrey Selian, 3G Mobile Licensing Policy: From GSM to IMT-2000 – A Comparative Analysis, available at <https://www.itu.int/osg/spu/ni/3G/casestudies/GSM-FINAL.pdf>.

to attract as many adoptors as possible as fast as they can – individually or within the framework of joint ventures and strategic alliances. Where one firm (or group of firms) succeeds, the said network effects, combined with first-mover-advantages, may induce a "lock-in" of the market into the first successful standard. More efficient standards that are introduced later on may fail.[34] In economics, this phenomenon is well-known as the problem of an inefficient market selection of technologies through dynamic effects (or path dependency effects).[35] However, even where the successful standard was optimal at the time of its introduction, it may become inefficient over time. The lock-in effects can be an important barrier for the replacement of the old standard with newer ones.[36]

24 However, if none of the firms is capable of securing a large advantage early on, so-called "standard wars" may emerge, in which the competing firms use bundling strategies, low pricing or preemptive strategies to fight competing standards and to achieve a "tipping" of the market in favor of their own standard. On the one hand, such competition may be advantageous because the market will not be locked into one standard early on. The extended period of competition between different standards can lead to the development of better standards. On the other hand, both the parallel experimentation with different standards and the uncertainty about the future standard can lead to wasteful investments and slow down the innovation on the market for complementary products and services.[37]

25 **Incentive problems of individual firms:** Since the firms that try to introduce a standard (or participate in a process of collective standard-setting) have different strengths and weaknesses with regard to their technological capabilities, their patent portfolios and/or their market positions, their incentives and strategies for choosing and introducing a particular standard can differ significantly. The private incentives for choosing a certain standard may not align with the social benefits. This is all the more true because a firm will usually not be able to internalize all the positive effects that a standard may have for other firms and consumers. The benefits of open interfaces, for example, will accrue to the many other firms that are thus enabled to develop complementary products or services, and, as a consequence, to consumers.[38] Due to this incentive problem, the market may end up in an equilibrium with too many different standards and isolated proprietary solutions. Such an excessive fragmentation is an important concern in the ongoing debates about standards in the digital economy.[39] Compared to such fragmentation, even the unilateral setting of a standard by a dominant firm may be preferable, as the dominant firm may be better able to internalize the benefits of such a standard and may therefore have greater incentives for choosing socially efficient standards. At the same time, the dominant firm may have socially inefficient incentives to stifle competition and innovation in markets for complementary products and services (ex-post competition) and to block innovation that may endanger its (long-term) market position.[40]

26 **Knowledge problems**: The development of new technical standards is in itself an innovation process that often takes place in the context of a rapid Schumpeterian technological evolution with disruptive innovations and a high degree of

34 In the interoperability discussion three different kinds of lock-in problems have to be distinguished. (1) Consumers can get "locked-in", because they buy a product or use a platform which require them to buy complementary products and services (as in aftermarkets) or because the products they buy on platforms cannot be transferred to other platforms (e.g., music files or e-books). (2) However, firms can also get "locked-in" into a standard or a system, if they have to make a standard- or system-specific investment for using the standard/system for their products and services. The patent hold up-problem in regard to standard-essential patents (Rambus case) as well as transaction-specific investments of app developers for Apple or Android (or component suppliers for car manufacturers) are well-known examples. (3) However, here we mean that also an entire market might be locked-in into a standard or technology due to the dynamic effects and path dependencies, which make it hard to replace the standards through a newer, more efficient one. For a sophisticated analysis of lock-in situations and strategies, see from a business perspective, Shapiro/Varian, Information Rules, 1999, 103-171.

35 See for these dynamic effects through network effects, first-mover advantages, path dependencies, and lock-in effects Katz/Shapiro, Network Externalitites, Competition and Compatibility, American Economic Review 75, 1985, 424; David, Clio and the Economics of QWERTY, American Economic Review 78, 1988, 332; Arthur, Competing Technologies, Increasing Returns, and Lock-In by Historically Small Events, in: Arthur, Increasing Returns and Path Dependence in the Economy, 1994, 13; Shapiro/Varian, Information Rules, 1999, 173-225.

36 In such a case of market failure different policy solutions can be considered for overcoming these lock-in effects, as, e.g., subsidies, public procurement or regulation.

37 For the analysis of standard wars, see Besen/Farrell, Choosing How to Compete - Strategies and Tactics in Standardization, Journal of Economic Perspectives 8, 1994, 117; Shapiro/Varian, Information Rules, 1999, 261-296. Stango, The Economics of Standard Wars, Review of Network Economics 3(1), 2004, 1-19.

38 For the problem of internalizing complementary externalities and thereby aligning private and social benefits of a standard, see Farrell/Weiser, Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age, Harvard Journal of Law and Technology 17, 2003, 85.

39 OECD, Data-Driven Innovation. Big Data for Growth and Well-Being, 2015, 192-194.

40 See Farrell/Simcoe, Four Paths to Compatibility, in: Peitz/Waldfogel, The Oxford Handbook of the Digital Economy, 2012, 34, 44-45.

uncertainty (as in the current digital revolution).[41] Therefore, it is hard or even impossible to reliably predict what the optimal technical standards for the next five or ten years may be, inter alia with a view to facilitating follow-on innovation (of complementary products and services). Both the firms and the state (or regulators) face this knowledge problem. This is why a decentralized bottom-up process that also encompasses a process of parallel experimentation with different new standards may be advantageous for finding better standards, even if, due to a longer period of competition between standards, some of the static advantages of a single standard may be lost. Hence, there may be a Schumpeterian trade-off between the static benefits of a single standard and the dynamic benefits of experimenting with different standards for finding better solutions (competition as a discovery process).[42] Another implication of the knowledge problem is that it is often not clear whether a single monopolistic standard is the most efficient solution with a view to a specific interoperability problem, or whether two or more different standards may coexist and compete with each other in the market. These knowledge problems have to be taken into account when assessing potential market failures and defining desirable policy solutions.

27 What conclusions can be drawn from a comparison between the three main ways of standard-setting, with a view to these problems and effects? The said problems – dynamic effects, the critical mass problem and the danger of lock-in into an inefficient standard – may argue against decentralized standard-setting: competition for the standard may turn out to be a lengthy and wasteful process, and result in an inefficient standard in the end. Where a dominant firm imposes a standard, this will come at the risk of distorted incentives for choosing standards that stifle ex-post competition and innovation.[43] Moreover, the absence of experimentation with different standards may lead to a premature lock-in into an inefficient standard.

28 Against this backdrop, collective standard-setting in standard-setting organizations (SSOs) may seem to be the preferable solution. Participation in standard-setting organizations is usually voluntary. Apart from that, SSOs can be organized (and therefore also work) very differently. Regardless of the precise procedure, the agreed upon standards will be the result of a negotiation process in which technical experts will typically play a crucial role. This increases the chances of identifying a high-quality standard.[44]

29 Yet, SSOs are affected by a number of problems themselves. Due to their specific patent portfolios or market positions, the participating firms will usually have different interests. The need for a consensus solution is no guarantee for finding the best standard. Negotiations can fail or suffer from lengthy delays. During the process, firms are free to exit, possibly trying to impose their own standard unilaterally in the market.[45] Where the search for a collective standard is successful and the standard is adopted by the market, monopoly problems may arise. In an effort to appropriate a significant part of the value of the standard, holders of standard-essential patents (SEP) may engage – and have, in the past, engaged – in hold-up strategies.

30 In spite of these well-known problems, and the cooperative nature of collective standard-setting notwithstanding, EU competition law has adopted a rather beneficial stance towards collective standard-setting. According to the Commission's Guidelines on the applicability of Art. 101 TFEU to horizontal co-operation agreements,[46] standardization agreements are usually considered to be pro-competitive, as they tend to promote the internal market, encourage the development of new and improved products or markets and ensure interoperability and compatibility to the benefit of consumers (para. 263). Therefore, where:

> *"participation in standard-setting is unrestricted and the procedure for adopting the standard in question is transparent, standardisation agreements which contain no obligation to comply with the standard and provide access to the standard on fair, reasonable and non-discriminatory terms will normally not restrict competition within the meaning of Article 101(1) [TFEU]".*

41 See for the interrelationship between standardisation and innovation also LaRouche/Overwalle, Interoperability standards, patents and competition policy, TILEC Discussion paper, 2014, pp.17.

42 See Hayek, Competition as a discovery procedure, in: Hayek, New Studies in Philosophy, Politics, Economics, and the History of Ideas, 1978, 179; for the advantages of parallel experimentation and diversity see Kerber, Competition, innovation, and maintaining diversity through competition law, in: Drexl/Kerber/Podszun, Competition Policy and the Economic Approach, 2011, 179.

43 Farrell/Simcoe, Four Paths to Compatibility, in: Peitz/Waldfogel, The Oxford Handbook of the Digital Economy, 2012, 34, 35.

44 Farrell/Simcoe, Four Paths to Compatibility, in: Peitz/Waldfogel, The Oxford Handbook of the Digital Economy, 2012, 34, 41.

45 For the problems of collective standard-setting see Farrell/Simcoe, Four Paths to Compatibility, in: Peitz/Waldfogel, The Oxford Handbook of the Digital Economy, 2012, 34, 40-44. For empirical studies on SSOs see Chiao/Lerner/Tirole, The Rules of Standard Setting Organizations: An Empirical Analysis, The RAND Journal of Economics, 38(4), 2005, 905, and Rysman/Simcoe, Patents and the Performance of Voluntary Standard Setting Organizations, Management Science 54(11), 2009, 1920.

46 OJ 2011 No. C 11/1.

31 It may be considered a complement to this pro-collective standard-setting strategy that the Commission has recently stressed its determination to address the monopoly problem potentially associated with standard-essential patents. A review of FRAND[47] licensing policies for SEPs shall ensure fair and easy access to the standard[48] and contribute to lower royalty demands.[49] In a legal and economic environment where collective standard-setting is considered key,[50] the Commission wants to reduce the uncertainty that currently exists with regard to who the relevant community of SEP holders is and with regard to the cost of access to the cumulated intellectual property rights (IPRs) needed to implement the standard, and it strives to clarify the methodology applied to calculate the value of the licensing terms and the regime regarding the settlement of disputes. According to the Commission, a "fast, predictable, efficient and globally acceptable licensing approach, which ensures a fair return on investment for SEP holders and fair access to SEPs for all players is needed" (ICT Standardisation Priorities, p. 13). As of now, it is still unclear however, which direction the Commission's efforts will take.[51] In the past, the Commission has been willing to use competition law (namely Art. 102 TFEU) to go against exploitative licensing fees for SEPs following a patent ambush.[52] Both the *Samsung* and the *Motorola* case have defined the preconditions under which a request of an SEP holder for an injunction may constitute an abuse of dominance.[53] Apart from these special settings, the framework within which SEP holders commit to license on FRAND terms has been defined (albeit not enforced) by the relevant SSOs. In the future, the EU Commission may consider linking the legal privilege for collective standard-setting in SSOs to the existence and active enforcement of a qualified FRAND policy.

32 But the EU's policy with regard to collective standard-setting is not limited to privileging and supporting market-driven cooperative standard-setting endeavors as a "bottom-up" approach. Being concerned that, at least in the ICT sector, standardization is increasingly taking place outside of Europe, potentially undermining European competitiveness,[54] the Commission finds that it cannot be left to industry stakeholders to decide in which areas to develop standards, and at what speed. Rather, the Commission is determined to "define missing technological standards that are essential for supporting the digitisation of our industrial and services sectors" and to actively mandate European standardization bodies for a speedy delivery of standards[55] in order to "ensure that ICT-related standards are set in a way that is more responsive to policy needs" and sufficiently fast.[56] According to the recently published ICT Standardisation Priorities,[57] open European standards for 5G communications,[58] for the IoT, for cybersecurity, big data and cloud computing will be core. In various areas, the new digital economy requires an "open platform approach that supports multiple application domains and cuts across silos". Open standards shall support the entire value chain and integrate multiple technologies (p. 7). In particular, the Commission is interested in such open platforms and standards in the area of eHealth, transport systems, including automated vehicles, smart energy and advanced manufacturing (p. 10 et. seq.). At the same time, the new standardization processes shall take into account the blurring of the boundaries between traditional sectors and industries, products and services. They shall consider safety needs, data

47 FRAND = fair, reasonable and non-discriminatory.

48 EU Commission, A Digital Agenda for Europe, Brussels, 19.5.2010, COM(2015)245 fin., p. 15, announcing a follow-up to the White Paper "Modernising ICT Standard Setting in the EU", COM(2009) 324.

49 EU Commission, A Digital Agenda for Europe, Brussels, 19.5.2010, COM(2015)245 fin., p. 15.

50 EU Commission, A Digital Single Market Strategy for Europe, Brussels, 6.5.2015, COM(2015)192 fin., p. 15.

51 The Commission Staff Working Document "Analysis of measures that could lead significant market players in the ICT sector to license interoperability information", Brussels, 6.6.2013, SWD(2013)209 fin., p. 15-16 has proposed a number of non-legislative measures, inter alia model licenses for interoperability information and guidelines for determining the value of interoperability information. The idea is to enhance transparency in the licensing market and minimize practical hurdles to licensing, in particular for SMEs.

52 EU Commission, Decision of 9.12.2009, Case COMP/38.636 – Rambus (decision based on Art. 9 Reg. 1/03).

53 ECJ, Judgment of 16.7.2015, Case C-170/13 – Huawei Technologies; EU Commission, Decision of 29.4.2014, Case AT.39939 – Samsung; Decision of 29.4.2014, Case AT.39985 – Motorola.

54 EU Commission, A Digital Single Market Strategy for Europe, Brussels, 6.5.2015, COM(2015) 192 fin., p. 15.

55 EU Commission, A Digital Single Market Strategy for Europe, Brussels, 6.5.2015, COM(2015) 192 fin., p. 15.

56 EU Commission, ICT Standardisation Priorities for the Digital Single Market, Brussels, 19.4.2016, COM(2016) 176 fin., p. 2-3.

57 EU Commission, ICT Standardisation Priorities for the Digital Single Market, Brussels, 19.4.2016, COM(2016) 176 fin.

58 EU Commission, Communication "5G for Europe: An Action Plan", Brussels, 14.9.2016, COM(2016) 588 fin.: A lack of coordination between national approaches would "create a significant risk of fragmentation and implementation of standards and would delay the creation of a critical mass for 5G-based innovation in the Digital Single Market" (p. 3). The EU Commission finds that "standards are of paramount importance to ensure the competitiveness and interoperability of global communication networks" (p. 7) and plans to "foster the emergence of global industry standards under EU leadership for key 5G technologies (radio access network, core network) and network architectures" (p. 7).

exchange, and privacy concerns simultaneously (p.3) – aspects that, today, are typically dealt with separately. From this perspective, the Commission's pro-collective standard-setting approach is not limited to addressing market failures. Rather, what resonates in these communications and statements is that European standard-setting is a pro-active trade and industrial policy.

33 While collective standard-setting certainly is an important route towards interoperability, the mixed experiences do not allow for the conclusion that it is the optimal solution from an economic perspective. Both economic theory and empirical studies suggest that all paths towards interoperability have advantages as well as disadvantages. All strategies can work well under certain circumstances and suffer from serious problems under others. According to Farrell/Simcoe, it may be advisable to allow for the parallel pursuit of, and experimentation with, all four interoperability strategies, instead of heavily relying on just one of them. Even hybrid solutions may evolve in the market place over time.[59] A cautious, market-friendly approach is all the more expedient in light of the technological revolution that we currently witness in the digital economy. The greater the knowledge problems, the more suitable a more decentralized "bottom-up" search for standards and other interoperability solutions may be. Adapters and converters may play an important role in such a discovery process (see chapter F.). The indubitable merits of a pro-active policy stance towards standardization in the digital economy notwithstanding, there is a risk that in a highly innovative and dynamic digital environment, such a push for speedy, top-down standardization may lock the European industry into premature standards.

D. Interoperability regulation in the field of electronic communications

34 In some areas, the EU has gone far beyond a voluntary pro-collective-standard-setting approach and has created a legal basis for mandating interoperability within the framework of a regulatory regime. The legal empowerment of national regulatory authorities (NRAs) to mandate access[60] to or interconnection[61] between physical electronic communication infrastructures[62] – and in the future possibly to mandate interoperability even between number-independent interpersonal communications services[63] – is arguably the best example.

35 From an economic perspective, such access/interconnection/interoperability requirements may have three different rationales. (1) Communication network operators may be dominant in a relevant market for access of downstream competitors to the network (or to elements of that network) and may have incentives to act anti-competitively in this market, e.g., through not granting access to (unbundled), non-duplicable elements of their networks, which are essential for competitors to offer telecommunication services themselves. Therefore, there may be inefficiently low vertical interoperability (see also section E.). (2) Horizontal interconnection obligations between communication network operators that ensure end-to-end connectivity across networks eliminate the danger that the market may "tip" towards the largest communication network due to network effects. Horizontal interconnection regulation will shift the network effects from the individual network to the level of all interconnected networks and can thereby prevent the emergence of dominant communication networks (with all their potentially problematic effects). (3) In contrast to the first two rationales, which relate to market failure problems with regard to competition, the goal to ensure end-to-end interconnectivity in electronic communications may also be grounded in a public universal service policy. Such a policy is not based on a pure economic efficiency rationale, but relies heavily on a political decision in favor of society-wide end-to-end connectivity. Beyond distributional reasons, universal service in electronic communications provides for a communication infrastructure that is considered essential for the functioning of the economy, democracy, and the entire society.

36 The network access and interconnection regime for the electronic communication sector is currently[64]

59 Farrell/Simcoe, Four Paths to Compatibility, in: Peitz/Waldfogel, The Oxford Handbook of the Digital Economy, 2012, 34, 48-50.

60 "Access" means the making available of facilities and/or services, to another undertaking, under defined conditions, on either an exclusive or non-exclusive basis, for the purpose of providing electronic communications services, cf. Art. 2 lit. (a) of the Access Directive 2002/19/EC.

61 "Interconnection" means the physical and logical linking of public communications networks used by the same or a different undertaking in order to allow the users of one undertaking to communicate with users of the same or another undertaking, or to access services provided by another undertaking, cf. Art. 2 lit. (b) of the Access Directive 2002/19/EC.

62 "Electronic communications network" means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, cf. Art. 2 lit. (a) of Directive 2002/21/EC.

63 Proposal for a Directive establishing the European Electronic Communications Code, Brussels, 12.10.2016, COM(2016) 590 fin.

64 In this context, see the proposed Directive establishing the European Electronic Communications Code, Brussels,

set out in the Access Directive 2002/19/EC. According to this directive, NRAs may impose access obligations upon network operators based on different legal norms. Art. 5 of the Access Directive allows for the imposition of (vertical or horizontal) access, interconnection and interoperability requirements on electronic communication network operators irrespective of their market power, if necessary to ensure end-to-end connectivity. As the irrelevance of dominance shows, the goal of this norm is not to fight abuses of market power. Rather, it shall promote "efficiency, sustainable competition, and [...] the maximum benefit to end-users" – a justification which points both to the elimination of network effects as a factor of competition between electronic communication networks and to a universal service rationale. Yet, in practice, the German national equivalent to Art. 5 of the Access Directive – § 18(1) TKG – has been of limited relevance so far.[65]

37 Art. 8(2) with Art. 12(1) of the Access Directive 2002/19/EC have been significantly more relevant. Based on these provisions, NRAs may impose a range of access obligations upon network operators found to possess "significant market power"[66] in a market that the Commission has found to potentially be in need of regulation, and "where the regulatory authority considers that denial of access or unreasonable terms and conditions having a similar effect would hinder the emergence of a sustainable competitive market at the retail level, or would not be in the end-user's interest". The duties that may be imposed range from a duty to negotiate in good faith with undertakings requesting access (Art. 12(1) lit. b) to a duty "not to withdraw access to facilities already granted" (Art. 12(1) lit. c), an obligation "to give third parties access to specified network elements and/or facilities, including unbundled access to the local loop" (Art. 12(1) lit. a), to "grant open access to technical interfaces, protocols or other key technologies that are indispensable for the interoperability of services or virtual network elements" (Art. 12(1) lit. e), "to provide specified services needed to ensure interoperability of end-to-end services to users, including facilities for intelligent network services or roaming on mobile networks" (Art. 12(1) lit. g). Again, the regulatory authority may impose access or interconnection duties to ensure either horizontal or vertical interoperability.

38 The linkage of these authorizations for intervention to a position of "significant market power", which is generally understood to be equivalent to market dominance within the meaning of Art. 102 TFEU, suggests a competition law rationale. Where a dominant network operator would refuse to grant access to (unbundled) elements of its network which are essential for competitors to offer telecommunication services themselves and which cannot be duplicated, the "essential facilities"-doctrine would suggest an abuse of dominance. It is much less obvious whether an obligation to ensure horizontal interoperability – i.e. interconnection between two in and by themselves complete networks – could be imposed under competition law. So far, the pure reliance on network effects to work to a dominant firm's benefit has not been considered an abuse.[67] Like Art. 5, Art. 8 with Art. 12 of the Access Directive may therefore be informed by the goal to prevent market tipping (see above) – a pro-competitive rationale, but with no firm basis in competition law. Furthermore, the ex-ante-regulatory remedy under Art. 8 with Art. 12 of the Access Directive is limited to electronic communications markets where dominance is particularly entrenched.[68]

39 Recent debates have evolved around a possible extension of the existing interoperability requirements for electronic communications network operators towards (dominant or even non-dominant) number-independent interpersonal communications services providers (e.g. WhatsApp[69])

12.10.2016, COM(2016) 590 fin. which shall replace the existing legal framework for electronic communications.

65 Neitzel/Hofmann, in: Spindler/Schuster, Recht der elektronischen Medien, § 18 TKG, para 1; Scherer, in: Arndt/Fetzer/Scherer/Graulich, TKG-Kommentar, § 18, para 2.

66 Equivalent to the competition law concept of market dominance – see Commission guidelines on market analysis and the assessment of significant market power under the Community regulatory framework for electronic communications networks and services, OJ 2002 No. C 165/03, p. 14 et seq., Ricke, in: Spindler/Schuster, Recht der elektronischen Medien, § 3 TKG, para 6; Kohrenke/Ufer, in: Geppert/Schütz, Beck'scher TKG-Kommentar, § 3, para 10.

67 For a case at the limit of antitrust law which may be considered to be a "horizontal interoperability" case see US Supreme Court, Aspen Skiing Co. v. Aspen Highlands Skiing Corp., 472 U.S. 585 (1985).

68 The Commission applies a 3-criteria-test to identify potentially relevant markets. Ex ante-regulation shall be considered only for markets with: (1) high and non-transitory barriers to entry; (2) a market structure that does not tend towards effective competition within the relevant time horizon; (3) a market failure that cannot be adequately addressed by competition law alone. See Commission Recommendation 2014/710/EU of 9 October 2014 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with 2002/21/EC, OJ 2014 No. L 295/79. The Commission Recommendation currently indicates four potentially relevant markets: (1) wholesale call termination on individual public telephone networks provided at a fixed location; (2) wholesale voice call termination on individual mobile networks; (3a) wholesale local access provided at a fixed location; (3b) wholesale central access provided at a fixed location for mass-market products; (4) wholesale high-quality access provided at a fixed location.

69 Discussing this question: Inge Graef, Mandating portability and interoperability in online social networks,

and upon social media platforms (e.g. Facebook[70]). As is the case with electronic communications networks, interoperability between interpersonal communications services providers or social media providers would ensure end-to-end connectivity. In addition, an interoperability requirement would exclude the possibility for a dominant platform in a market characterized by tipping tendencies to function as "closed communities". Network effects so far working in favor of the dominant platform would benefit all like platforms as well.[71]

40 It is arguably along this logic that Art. 59(2) lit. c of the Draft European Electronic Communications Code[72] now proposes to introduce a new legal basis for NRA's intervention. According to this draft provision, NRAs shall be able to impose:

> *"in justified cases, obligations on providers of number-independent interpersonal communications services to make their services interoperable, namely where access to emergency services or end-to-end connectivity between end-users is endangered due to a lack of interoperability between interpersonal communications services".*[73]

41 The extension of horizontal interoperability regulation from physical infrastructures to interpersonal communications services and digital platforms is, however, not at all obvious. The balance of interests differs significantly. Neither the goal to prevent market tipping nor the universal service rationale are relevant across the board when it comes to digital platforms. Universal services policies strive to ensure a basic service – but not end-to-end connectivity in any possible respect. Interventions into the digital platform operators' freedom to choose between closed and open systems lacks justification where end users typically engage in multi-homing and thereby ensure de facto end-to-end connectivity themselves. Similarly, where multi-homing is common, tipping may not be an issue. Even where tipping may be a concern, the imposition of interoperability duties upon digital platforms may imply a significantly more interventionist regime than the interconnection requirement between physical networks. It is therefore important to clearly distinguish between network interconnection and platform interoperability.

42 Network interconnection is essentially limited to enabling an unhindered transmission of signals across well-defined technical interfaces. There is no need to regulate the resulting forms of communication or services. Physical network operators will normally not be responsible for regulating the content exchanged. Mandating horizontal interoperability between number-independent interpersonal communications services is an entirely different matter. The difficulty starts with determining what exactly interoperability shall mean. Interpersonal communications services operators may allow for the exchange of very different forms of data and content. In such a case, open interfaces may not be enough for ensuring end-to-end connectivity. Along which parameters and according to what rules shall users of different services be able to communicate? Which functionalities must be available? Which formats and user interfaces shall be used? Which legal authority will a service provider have over "external" users' speech? Likely, full horizontal interoperability can only be realized based on a high degree of standardization and/or horizontal cooperation between competitors. The degree of services differentiation will then suffer – a high price to be paid in an innovative, dynamic market setting with frequently changing business models and market boundaries.[74] A harmonization

Telecommunications Policy 2015 (39/6), 502 et seq.

70 See, for example, Ian Brown/Christopher Marsden, Regulating Code: Good Governance and Better Regulation in the Information Age, 2013, pp. 190-191 who have argued in favour of imposing interconnection requirements on social network providers.

71 In favour of an interoperability requirement for these reasons: Graef/Valcke, Exploring new ways to ensure interoperability under the Digital Agendy, Info – the journal of policy, regulation and strategy for telecommunications, information and media 2014 (16/1), p. 7: "In early phases of market development, a duty to disclose interoperability information should only be mandated in very limited circumstances, since in this period competition between systems could be particularly beneficial for innovation. In later stages of market development, the need for mandated interoperability increases as the prevailing system continues to dominate the market."

72 Proposal for a Directive establishing the European Electronic Communications Code, Brussels, 12.10.2016, COM(2016)590 fin.

73 Art. 59(2) lit. c of the Draft European Electronic Communications Code is further qualified in Art. 59(3). According to this provision, obligations under Art. 59(2) lit. c may only be imposed "(i) to the extent necessary to ensure interoperability of interpersonal communications services and may include obligations to the use and implementation of standards or specifications ...; (ii) where the Commission on the basis of a report that it had requested from BEREC, has found an appreciable threat to effective access to emergency services or to end-to-end connectivity between end-users within one or serveral Member States or throughout the European Union and has adopted implementing measures specifying the nature and scope of any obligations that may be imposed ...".

74 Arguably for this reason, a Commission Staff Working Paper that discussed the expedience of an "Interoperability Directive", namely the imposition of an interoperability requirement not only upon electronic communications networks, but also on digital platforms and services considered exceptions to compulsory licensing that should apply "where the interoperability information (like the description of a hardware interface) reveal to a large extent the technology and functionality implemented by a device or a system beyond its interfaces" – see Commission Staff Working Document, Analysis of measures that could lead significant market players in the ICT sector to license

of contractual rules may even be required to make the regime manageable.[75] Such an interoperability regulation is likely to affect investment choices by the dominant network operator and its competitors in potentially complex ways.

43 Given these concerns, a strong justification for mandating horizontal interoperability will be needed. The universal service logic that applies to the interconnection of physical electronic communications networks should not be easily extended to all types of communication services. A severe form of market failure and/or policy need should be clearly identified. Measures less intrusive than the imposition of interoperability must be unavailable. Frequently, a widespread practice of multi-homing or the availability of "adapters", i.e. of instruments that allow users to overcome interoperability hurdles unilaterally, will provide for an acceptable level of connectivity.

44 These restrictions to any interoperability requirement are set out only incompletely in the new Art. 59(2) lit. c of the Draft European Electronic Communications Code. The breadth of regulatory necessities implicated by an extended interoperability policy for number-independent interpersonal communications services should caution against the introduction of such a provision, or at least against its future application by NRAs.

E. Horizontal and vertical interoperability in the case of dominant firms

45 In section C., we showed that we cannot expect market forces to bring about efficient interoperability solutions in the presence of a dominant market player: the market outcome may not properly match the trade-offs between the advantages of more interoperability and the advantages of more differentiation that less interoperable and more "closed" systems may allow for. Some extent of market failure with regard to optimal degrees of horizontal and vertical interoperability may emerge. We shall now inquire how competition law can address the resulting market failures. Is competition law – and in particular Art. 102 TFEU – available where competition fails to control a dominant digital platform's unilateral "closed" business strategy – both with regard to horizontal and vertical interoperability?[76]

I. Horizontal interoperability

46 Horizontal interconnection / interoperability denotes the ability of horizontally competing networks, services or platforms to interact with one another (see above). As the example of electronic communications networks has shown, interconnection / interoperability requirements can prevent market tipping, since network effects will no longer work in favor of the strongest player alone, but will be market-wide. While this, together with a universal service rationale, has been a justification for the imposition of regulatory duties, the question is whether a refusal to interconnect with a horizontal competitor could qualify as an abuse under Art. 102 TFEU – and consequently justify the imposition of interoperability duties as a competition law remedy. There is, however, only one single precedent – a precedent from US antitrust law – for the imposition of such a duty to cooperate horizontally, namely the *Aspen Skiing* case.[77] In US law, the *Aspen Skiing* case is highly controversial[78] and known to lie at the "outer boundary" of antitrust liability.[79] Under EU competition law, the refusal to interconnect horizontally has not yet been found to constitute an abuse. The fact that a dominant firm benefits from network effects does not qualify as an abuse, nor does the risk of market tipping change this legal appraisal. From an economic perspective, a duty to interoperate at the horizontal level would risk to replace competition for innovation and differentiation by mere price competition between homogeneous products and services. It is not for competition law to impose such choices.

47 Instead of mandating horizontal cooperation, EU law has, in various contexts, opted for an alternative and significantly less intrusive instrument to increase competition: Both Art. 20 of the General Data Protection Regulation 2016/679,[80] and Art. 16(4) lit.

interoperability information, SWD(2013) 209 final, p. 12.

75 For a discussion also see Inge Graef, Mandating portability and interoperability in online social networks, Telecommunications Policy 2015 (39/6), 502, 510 et seqq.

76 In this article we will not discuss the difficulties in determining whether a firm and especially a (multi-sided) platform is dominant (including the difficulties of defining markets). These difficulties may further limit the capability of competition law to properly solve interoperability problems.

77 US Supreme Court, Aspen Skiing Co. v. Aspen Highlands Skiing Corp., 472 U.S. 585 (1985).

78 Critical with regard to Aspen Skiing: John E. Lopatka/ William H. Page, Bargaining and Monopolization: In Search of the 'Boundary of Section 2 Liability' between Aspen and Trinko, Antitrust Law Journal 82 (2005), pp. 115 et seq.; Alan J. Meese, Property, Aspen, and Refusals to Deal, Antitrust Law Journal 73 (2005), pp. 81 et seq. In favour of a broader reading of *Aspen Skiing*: Marina Lao, Aspen Skiing and Trinko: Antitrust Intent and 'Sacrifice', Antitrust Law Journal 73 (2005), pp. 171 et seq.

79 Verizon Communications v. Law Offices of Curtis V. *Trinko,* LLP, 540 *U.S.* 398 (2004).

80 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, OJ 2016 L 119/1. See also: Article 29 Data Protection Working Party, Guidelines on the

b of the Draft Directive on Digital Content[81] set out a duty to ensure data portability.[82] Data portability requires some degree of interoperability between different data formats, but does not presuppose full interoperability. While data portability – contrary to interoperability – does not overcome network effects that may work in favor of one particularly prominent platform, it may ease any data-induced lock-in effect. By increasing user mobility, a coordinated move to superior alternatives is facilitated. Market barriers to entry are not eliminated, but reduced.

48 Similarly, the ability of dominant firms to enter into exclusivity agreements with customers will be subject to significant constraints under Art. 102 TFEU, as such agreements will impose additional switching costs upon customers and thereby reduce competition.

II. Vertical interoperability

49 A dominant firm (or platform) may also have incentives to foreclose competition on adjacent markets by hampering interoperability with third party complementary products and services.[83] As users will frequently place a premium on interoperability, such conduct may have the potential to leverage market power from the platform market to neighboring markets. In order to protect competition and follow-on-innovation on such adjacent markets, mandating vertical interoperability may be economically justified.[84] At the same time – as already discussed in the context of network interconnection regulation – mandating access to interfaces or platforms may negatively affect the innovation and investment incentives of the dominant firm at the platform/systems level. Also, there may be valid efficiency justifications for a closely controlled interface (or platform), such as, *inter alia*, quality, safety, and security concerns.[85] The economically optimal degree of vertical interoperability will depend on the specific circumstances of a case.

50 This is the complex economic dilemma underlying the so-called "essential facilities" doctrine. On the basis of this doctrine – well established in EU competition law, but treated with much more skepticism in US antitrust law – a refusal to grant access to interface information has been qualified as an abuse of dominance in the *Microsoft* case.[86] In 2004, the EU Commission ordered Microsoft to make available to its competitors on the work group server market interoperability information regarding the interface with Microsoft's client PC operating system. Microsoft had freely provided this information to third parties for some time. After entering the work group server market itself, and having gained some experience with this product, it had ceased to do so in 1998 however.[87] Microsoft's competitors on the work group server market tried to maintain some level of compatibility between their software and Microsoft's client PC operating system based on re-engineering techniques. Yet, the degree of compatibility – and hence the quality and utility of their workgroup server software for users – was significantly reduced. In order to compete effectively in the work group server market, competitors needed full access to Microsoft's interface specifications. According to the Commission, under these circumstances Microsoft's refusal to disclose the relevant interface information to competitors constituted an abuse of Microsoft's dominant position on the market for client PC operating systems. The protection of the relevant interface information by alleged IPRs did not justify Microsoft's refusal to disclose, as this refusal significantly hampered follow-on innovation and competition on quality in the market for work group servers. Microsoft had limited the technical development to the prejudice of consumers. In 2007, the GC upheld the Commission's decision.[88]

51 Much of the controversy that has followed this judgment has concerned its precedential value.[89] The ECJ's broad interpretation of the criteria for finding an abuse of dominance under the so-called "essential facilities" doctrine has the potential to significantly overstretch the doctrine's reach in future cases. GA Jacobs, by contrast, has famously called for a narrow construction of the "essential facilities" doctrine in

right to data portability, adopted on 13 December 2016, 16/EN WP 242.

81 Draft Directive on certain aspects concerning contracts for the supply of digital content, 9 December 2015. COM(2015)634 fin.

82 See Ruth Janal, Data Portability, p. 59 in this issue.

83 John M. Newman: Anticompetitive Product Design in the New Economy, Florida State University Law Rev. 39 (2012), pp. 1, at 14.

84 For a discussion of arguments in favour of mandating interoperability see Fleischer, Behinderungsmißbrauch durch Produktinnovation, 1997, § 3.

85 See Fleischer, Behinderungsmißbrauch durch Produktinnovation, 1997, § 4.

86 EU Commission, Decision of 21 April 2004, COMP/C-3/37.792 – Microsoft; CFI, Judgment of 17.9.2001, Case T-201/04 – Microsoft Corp.

87 For a critical economic assessment of this conduct see Leveque, Innovation, Leveraging and Essential Facilities: Interoperability Licensing in the EU Microsoft Case, World Competition 28(1), 2005, 71, 82-85; see also Kühn / Van Reenen (2009), Interoperability and Market Foreclosure in the European Microsoft Case, in: Lyons, Cases in European Competition Policy: The Economic Analysis, 50.

88 CFI, Judgment of 17.9.2001, Case T-201/04 – Microsoft Corp.

89 See, for example, Daniel F. Spulber, Competition Policy and the Incentive to Innovate: The Dynamic Effects of Microsoft v. Commission, Yale Journal of Regulation 25 (2008), pp. 247, 272 et seq.

an earlier case:[90]

> *"In the long term it is generally pro-competitive and in the interest of consumers to allow a company to retain for its own use facilities which it has developed for the purpose of its business. For example, if access to a production, purchasing or distribution facility were allowed too easily there would be no incentive for a competitor to develop competing facilities. Thus while competition was increased in the short term it would be reduced in the long term. Moreover, the incentive for a dominant undertaking to invest in efficient facilities would be reduced if its competitors were, upon request, able to share the benefits. Thus the mere fact that by retaining a facility for its own use a dominant undertaking retains an advantage over a competitor cannot justify requiring access to it." (para. 57)*

52 In fact, the Commission, in its *Microsoft* decision, had tried to consider this concern. Addressing Microsoft's argument that an obligation to disclose its allegedly IP-protected interface information would reduce its future incentives to innovate, the Commission had proposed an "incentives balance test": a refusal to license should be justified if the resulting innovation incentives for the dominant firm would outweigh the loss of innovation by rival firms on the adjacent market. In the *Microsoft* case, the Commission had found the overall innovation activities in the industry to be larger with than without mandatory disclosure of interface innovation, however.[91]

53 Economically, this balance test restates the difficult trade-off between the different innovation incentive effects of open versus closed interfaces.[92] Nonetheless, the GC did not endorse this balance test. It is the task of the law to translate economic insights of the relevant trade-offs into legally manageable criteria that allow for a certain degree of predictability and legal certainty. In the absence of economic methods that allow for a reliable quantification of these innovation incentive effects, an incentives balance test cannot be expected to render objective, predictable results.

54 Unfortunately, the *Microsoft* judgment does not offer an alternative test that would sensibly limit the application of the doctrine to other interoperability cases either. The lack of conceptual clarity regarding the "essential facilities" doctrine as it now stands complicates its transposition to the relatively new and not yet fully understood phenomenon of digital platforms. Strong concentration tendencies in platform markets might seem to justify a pro-active imposition of interoperability obligations at first sight – a measure of comparatively low intrusiveness, but suitable to effectively prevent a long-standing monopoly. Interestingly, the Commission's 2005 Discussion Paper on Exclusionary Abuses suggested such a line of reasoning.[93] While the Commission highlighted that there "is no general obligation even for dominant companies to ensure interoperability", it proposed to assume an abuse wherever a dominant company withheld the relevant interface information to leverage market power from one market to another. Even if the relevant information were protected by a trade secret, it might "not be appropriate to apply to such refusals to supply information the same high standards for intervention" as they have been established for refusals to provide access more generally.

55 This passage has not made its way into the Commission's final Guidance Paper on exclusionary abuses, which was published in 2009.[94] In substance, it has downplayed the context-sensitivity of interoperability. Current discussions on the application of the "essential facilities" doctrine to digital platforms rather question its suitability in a context which significantly differs from the traditional setting of physical infrastructures.[95]

56 An example for such caution in imposing interoperability remedies is the French Conseil de la Concurrence's refusal to order Apple to license its Digital Rights Management (DRM) technology FairPlay to VirginMega, one of its competitors in the market for music download services.[96] Apple tried to tie iPod users to its own music download service iTunes by using its proprietary Fairplay technology, refusing to support rival standards on its iPod, and

90 Opinion of Advocate General Jacobs, Bronner, Case C-7/97, [1998] E.C.R. I-7794, at paras. 56-58.

91 See EU Commission, Decision of 21 April 2004, COMP/C-3/37.792, at para. 783 – Microsoft.

92 See Leveque, Innovation, Leveraging and Essential Facilities: Interoperability Licensing in the EU Microsoft Case, World Competition 28(1), 2005, 71, 75-78, who offers convincing arguments why from an economic perspective the incentives balance test is conceptually clearer than the new product test, and therefore might be preferable. For an analysis of the incentive balance test particularly from an innovation economics perspective see Vezzoso, The Incentives Balance Test in the EU Microsoft Case: A Pro-Innovation "Economics-Based" Approach? In: European Competition Law Review 27, 2006, 382, and Schmidt/Kerber, Microsoft, Refusal to License Intellectual Property Rights, and the Incentive Balance Test of the EU Commission, 2008 (available at SSRN: <http://ssrn.com/abstract=1297939>).

93 DG Competition, Discussion Paper on the application of Article 82 of the Treaty to exclusionary abuses, Brussels, December 2005, paras. 241, 242.

94 EU Commission, Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, OJ 2009 No. C 45/7.

95 See, for example, Bundeskartellamt, Digitale Ökonomie – Internetplattformen zwischen Wettbewerbsrecht, Privatsphäre und Verbraucherschutz, 1. October 2015, p. 29.

96 Conseil de la Concurrence, Décision No. 04-D-54 du 9 Novembre 2004 relative à des pratiques mises on oeuvre par la société Apple Computer, Inc. dans les secteur du Téléchargement de musique sur Internet et des baladeurs numériques. See also: Graef/Valcke, p. 6.

refusing to license FairPlay to competitors in the music download services market. VirginMega's request for a Fairplay license to expand its user base was denied. Yet, the Conseil de la Concurrence found that, irrespective of a possible position of dominance of Apple on the markets for portable music players and downloaded music, access to Apple's DRM technology was not indispensable for operating a music download service. Among the core arguments was the possibility for users to create compatibility themselves, namely by converting the format of VirginMega's downloaded music into Apple's ("ripping"). The cost of doing so was negligible, and it was a commonly used method. Also, several alternative portable music players were available on the market, all of which were compatible with VirginMega's DRM technology. Finally, the Conseil de la Concurrence was convinced by Apple's argument that licensing FairPlay to VirginMega would have weakened its security system, contrary to its contractual commitments to the recording industry.

57 This case once again illustrates the potential complexities of imposing interoperability duties on digital platforms, not only in horizontal, but also in vertical settings. Interoperability that extends beyond a purely technical level may raise issues of contractual and non-contractual liability and of security, and may consequently go along with heightened monitoring requirements. There may be valid business reasons not to allow for interoperability with competing platforms, but to operate a closed community. Here, like in the case of horizontal interoperability, data portability may be a preferable instrument for promoting competition (see above).

F. Hurdles for unilateral interoperability solutions

I. Adapters and converters as unilateral interoperability solutions

58 A very important (and in the discussion so far underestimated) group of solutions to interoperability problems are unilateral solutions. Firms that want to link up to a "closed" system, or that want to enable their users to link up, can create and offer adapters or converters that achieve (full or limited) interoperability with the "closed" platform or a system without that platform's active cooperation. In effect – depending on the degree of their perfection – adapters or converters may be able to eliminate the "natural monopoly" situation of a single uniform standard (see above, C.) and allow for the coexistence and competition between different standards, thus reviving the market mechanism for finding optimal or replacing outdated standards. Irrespective of standardization, adapters and converters can solve many of the interoperability problems associated with the horizontal and vertical openness of platforms and other closed systems.[97] Adapters and converters may also facilitate portability, thereby reducing switching costs and lock in-problems of consumers and firms, or help to solve aftermarket problems. The decentralized and bottom up invention of adapters and converters can promote innovative solutions for a wide array of interoperability problems.

59 As adapters and converters may seriously challenge a firm's business choice in favor of a "closed" system, such firms may have strong incentives to obstruct the well-functioning of such interoperability solutions, however, thereby re-establishing the users' lock-in.[98] Possible instruments of obstruction range from the technical design of interfaces such as to hamper the unilateral interoperability solutions to a frequent change of interfaces or pro-active blockages.[99] Facebook for example, has been said to actively block Google Chrome's extension for exporting friends, thereby reinforcing the lock-in of Facebook users. In order to ward off decompilation efforts by competitors on the core market or neighboring markets, dominant companies may integrate so-called "obfuscators" into their software to complicate the attempt to access interface information.[100] In a more recent proceeding against

97 For the economic analysis of the role of adapters and converters in standardization contexts, see David/Bunn, The economics of gateway technologies and network evolution: Lesson from electricity supply history, Information economics and policy 3, 1988, 165, Farrell/Saloner, Converters, compatibility, and the control of interfaces, Journal of industrial economics 40, 1992, 9, Farrell/Simcoe, Four Paths to Compatibility, in: Peitz/Waldfogel, The Oxford Handbook of the Digital Economy, 2012, 34, 46-47, and Kölln, Strategien der Diffusion von Netzwerkgütern, 2013 (Dissertation), 123 et seq.

98 Farrell/Simcoe, Four Paths to Compatibility, in: Peitz/Waldfogel, The Oxford Handbook of the Digital Economy, 2012, 34, 47; Shapiro/Varian, Information Rules, 1999, 281 et seq.

99 See, for example, John M. Newman: Anticompetitive Product Design in the New Economy, Florida State University Law Rev. 39 (2012), pp. 1, 3, 15.

100 Commission Staff Working Document: "Analysis of measures that could lead significant market players in the ICT sector to license interoperability information", Brussels, 6.6.2013, SWD(2013)209 fin., p. 13-14, 19, pointing to the example of Microsoft's Windows Server Protocols (WSPP): almost a decade of reverse engineering (through protocol analysis) and development by the free/open source Samba project did not yield a fully compatible implementation of the protocols. The licensing of the WSPP by Microsoft was ultimately necessary for achieving full interoperability.

Google, the Commission is concerned that Google has contractually restricted software developers in the offering of tools that allow for a seamless transfer of search advertising campaigns across different search engines.[101]

60 Competition law may have to take a stance on such actions when it is a dominant firm that engages in such behavior. The said strategies can reduce competition and innovation of complementary products and services, and thereby reduce social welfare and harm consumers. Any competition law analysis will have to consider the potential costs of adapters and converters however. While the protection of differentiation may not be a central concern in a dominance setting, even dominant firms may legitimately strive for a higher degree of quality and/or security by opting for a "closed" system. The invention of adapters and converters can also weaken the closed system operator's innovation incentives and create free-rider problems. Competition law – as well as IP and trade secret law – may want to take account of the finding that in certain settings, certain strategies for defending the "closedness" of a platform or a system may be economically justified

II. "Interoperability obstruction" as an abuse of dominance?

61 From a competition law perspective, adapters and converters, wherever they emerge in the presence of a dominant platform or system, seem to hold the promise to significantly revive competition, and may be relevant in two important respects. Firstly, a non-interoperability policy of a dominant platform or system should not be considered abusive if sufficiently effective means are available to competitors or users to achieve interoperability themselves. In the *Apple FairPlay* case, the Conseil de la Concurrence considered the possibility to convert the music files into a different format in this spirit. Any means that enables competitors and/or users to solve the interoperability problem themselves should be considered before imposing access remedies.

62 Secondly, an obstruction of such market-driven interoperability solutions by the dominant player may constitute an abuse under Art. 102 TFEU. In the US, the 9th Circuit Court refused to qualify MySpace's decision to redesign its social media platform such that individual users were no longer able to link to content of competing social media platforms as an unlawful monopolization.[102] While MySpace was the dominant social media platform in the US at the time, the 9th Circuit Court did not find either exclusionary conduct or causal antitrust injury. A refusal to deal claim failed because, according to the Court's reasoning, there was no prior course of dealing between MySpace and its competitors; if at all, there had been a prior course of dealing between MySpace and its users. Moreover, the plaintiff had not shown that any prior course of dealing had been profitable to MySpace, such that its termination was contrary to MySpace's interest. The fact that MySpace's conduct prevented consumers from accessing competitors' websites through MySpace did not suffice for finding an antitrust injury. It is unclear whether this case would have been decided similarly in the EU.

63 At the same time, it is notoriously difficult to deal with practices by which dominant firms frequently change the configuration of relevant interfaces and thereby frustrate attempts by competitors to access interface information by way of reverse-engineering. While such changes may boil down to raising rivals' costs strategies, they may also qualify as legitimate product innovation or security measures.[103] In ambivalent cases, the outcome will frequently depend on the structure of the legal rule that is applied to such conduct: namely (1) on the division of the burden of proof; and (2) on whether the relevant conduct of a dominant firm should be subject to a proportionality principle. In the US, courts have proposed different tests under Sec. 2 Sherman Act. According to one line of cases, the implementation of a product change by a dominant firm will not be considered anti-competitive whenever the dominant firm can show some degree of innovation or product improvement.[104] No balancing of the benefits of product improvement versus anti-competitive effects shall apply, as courts would be unable to administer such a balancing exercise.[105] In *United States v. Microsoft Corp.*, by contrast, the Court of Appeals – District of Columbia

101 EU Commission, Press Release of 14 July 2016, IP/16/2532.

102 *LiveUniverse, Inc. v. MySpace, Inc.*, No. 07-56604, 2008 WL 5341843 (9th Cir. Dec. 22, 2008).

103 See Holger Fleischer, Behinderungsmißbrauch durch Produktinnovation, 1997, § 4; John M. Newman: Anticompetitive Product Design in the New Economy, Florida State University Law Rev. 39 (2012), pp. 1, 2 et seq.

104 See Berkey Photo, Inc. v. Eastman Kodak Co., 603 F. 2d (1979 U.S. App.), 286, 287; Allied Orthopedic Appliances Inc. v. Tyco Health Care Group L.P., 592 F.3d 991; 2010 U.S. App., 1000.

105 Allied Orthopedic Appliances Inc. v. Tyco Health Care Group L.P., 592 F.3d 991; 2010 U.S. App., 1000: "There is no room in this analysis for balancing the benefits or worth of a product improvement against its anticompetitive effects. If a monopolist's design change is an improvement, it is necessarily tolerated by antitrust laws. To weigh the benefits of an improved product design against the resulting injuries to competitors is not just unwise, it is unadministrable. There are no criteria that courts can use to calculate the right amount of innovation which would maximize social gains and minimize competitive injury."

Circuit has proposed a somewhat different test: where likely anti-competitive effects are established, the analysis will not end with the proposition of an "innovation" or "product improvement defense". Rather, in reaction to an alleged pro-competitive justification, any plausible pro- and anti-competitive effects need to be analyzed within the framework of a "balancing enquiry".[106] US academics are divided along similar lines: some have argued for a strong presumption in favor of the legality of any type of product innovation,[107] while others have supported the *Microsoft* balancing test.[108]

64 Within the EU, no clear test for "interoperability obstruction" has evolved as of now.[109] In the European *Microsoft* case – which could have been considered a case of interoperability obstruction – the GC applied the ill-suited "essential facilities" doctrine instead (see above). A broader view of the European case law would suggest that the proportionality principle will play a significantly larger role in the EU as opposed to the US. The challenge how to structure the balancing of anti- vs. pro-competitive effects on competition such that the consequence is a manageable and predictable test has not been met so far. Shifting focus from access to interoperability information to addressing potentially anti-competitive strategies of interoperability obstruction appears to be the next and much-needed step in developing a sound pro-interoperability strategy for the digital age.

III. Protection of decompilation in IP and trade secret law

65 Where the lack or inadequacy of (horizontal or vertical) interoperability between products and/or services is due to the non-availability of software interface information, the evolution of market-driven remedies may be promoted by efforts of market actors to decompilate the relevant software. Decompilation denotes the process by which a machine executable program is analyzed and translated back into the original source code.[110] Where the software proprietor refuses to grant access to relevant interface information, third-party decompilation may allow for its extraction, and may thereby allow producers of complementary software or products to ensure or improve interoperability.[111]

66 Decompilation involves the copying of the relevant software. Therefore, where the relevant software is protected by a copyright, the prior approval of the right holder may be needed. While ideas and principles are not protected by copyright law, the process used to identify these ideas and principles may infringe copyrights. Art. 6 of the Software Copyright Directive[112] provides for an exception however, where decompilation is used with the aim to achieve interoperability. The precise structure of this exception is the result of a hard-fought battle between lobbying groups,[113] which was ultimately won by the advocates of a rather restrictive exception. In order to rely on the exception, the person undertaking the decompilation must have a license or a right to use the program; decompilation must be "indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs"; this indispensable information must not have been previously available to the person performing the decompilation; and decompilation must be confined to the parts of the original program which are necessary to achieve interoperability. Where these conditions are met, the Software Copyright Directive does not distinguish between horizontal and vertical interoperability: decompilation is then permissible in both cases. However, the ECJ, in its *SAS* judgment, has found that the information obtained by way of decompilation must not be used "for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright."[114]

67 Where some of the preconditions for the decompilation exception in Art. 6 of the Software Copyright Directive, like the indispensability criterion and the proportionality criterion, seem to be informed by the "essential facilities" doctrine; both the preconditions for the permission and the content of the permission differ substantially: Art. 6 does not presuppose market dominance. At the

106 Microsoft III, 253 D. 3d 34, 47 ff. (D.C. Cir. 2001).

107 George Sidak, Debunking Predatory Innovation, Columbia Law Review, Vol. 83 (1983), p. 1148. In the context of product switching in the pharma sector: Douglas H. Ginsburg/Koren W. Wong-Ervin/ Joshua D. Wright, Product Hopping and the Limits of Antitrust, CPI Antitrust Chronicle, Dec. 2015(1).

108 John M. Newman: Anticompetitive Product Design in the New Economy, Florida State University Law Rev. 39 (2012), pp. 1 et seq. See also: William H. Page/ Seldon J. Childers, Antitrust, Innovation and Product Design in Platform Markets: Microsoft and Intel, in Antitrust Law Journal 78 (2012), pp. 363 et seq.

109 For an analysis of the relevant case law see Holger Fleischer, Behinderungsmißbrauch durch Produktinnovation, 1997, § 6 II.

110 Commission Staff Working Document: "Analysis of measures that could lead significant market players in the ICT sector to license interoperability information", Brussels, 6.6.2013, SWD(2013)209 fin., p. 13.

111 Wiebe, Interoperabilität von Software, Jipitec 2011, p. 89, 90.

112 Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs. For the German implementation of Art. 6 see § 69e UrhG.

113 Wiebe, Interoperabilität von Software, Jipitec 2011, p. 89.

114 ECJ, 2 May 2012, C-406/10, at para. 60 – SAS.

same time, Art. 6 does not burden the right holder with a duty to actively provide access or public information, but is limited to a duty to tolerate.

68 The exception provided for in Art. 6 of the Software Copyright Directive has been extended to the unified patent. According to Art. 27(k) of the Agreement on a Unified Patent Court, the rights conferred by European patents with unitary effects will not extend to the use of information obtained through the acts allowed under Article 5 and 6 of the Software Copyright Directive, in particular by its provisions on decompilation and compatibility. Likewise, the acquisition of a trade secret is considered lawful when the trade secret is obtained by "observation, study, disassembly or testing of a product or object ... that is lawfully in the possession of the acquirer of the information".[115] However, the use of a trade secret shall be unlawful, where it is carried out in breach of a confidentiality agreement or a contractual duty to limit the use of the trade secret (Art. 4(2) lit. b and c of the Trade Secret Directive). The trade secret exception can therefore easily be overridden by the right holders' licensing terms.[116]

69 While these IP law exceptions seem to open a different, market-driven path towards interoperability, it is not completely clear how useful these exceptions are in practice in helping to overcome the hurdles erected by non-interoperability business strategies. Obviously, the exceptions will not help where the relevant software is not available to other market actors, but runs only on servers of the software proprietor (so-called Application Service Providing – ASP). Secondly, software proprietors frequently engage in code obfuscation in order to hinder decompilation. Code obfuscation implies a deliberate modification of the relevant code meant to hamper its understanding.[117] In principle, it will not completely preclude decompilation, but it can significantly complicate and make it economically unattractive for all practical purposes.[118] Apart from obstructing competitors in their decompilation efforts, such a practice may also function as a prima facie legitimate security measure.[119] It cannot be easily prohibited therefore.[120] Finally, the IP exceptions have been criticized for being too narrowly construed.[121] Along this line, the Commission Staff Working Paper on interoperability has discussed whether interoperability information should be protected by copyright at all.[122] A number of scholars have argued in favor of a general permission of reverse engineering.[123] The rights holder's legitimate interest in retaining a competitive lead will be protected nonetheless by the fact that re-engineering of complex interface information is time-consuming and costly for competitors.[124] The "interoperability exception" may continue to be limited to those cases where the competing software does not contain identical or very similar expression. Furthermore, more discussion will be needed on the limits of the interoperability permission in cases where the interoperability information reveals to a large extent the technology and functionality implemented by a device or a system beyond its interfaces, or allows access to such functionality.

70 Overall, a search for market-driven solutions to interoperability hurdles should certainly include a renewed discussion on the optimal construction of an IP exception for interoperability information. However, while a significantly broadened exception could be an element of a pro-interoperability policy, it will not provide a general solution. It would need to be flanked by a competition policy that would actively address the anti-competitive obstruction of market efforts to overcome interoperability hurdles

.

115 Art. 3(1) of the Trade Secret Directive 2016/943 of 8 June 2016, OJ 2016 L 157/1.

116 Before the entry into force of the Trade Secret Directive, it was believed that trade secret protection cannot be invoked against the use of interoperability information obtained through lawful reverse engineering and decompilation – see Commission Staff Working Document: "Analysis of measures that could lead significant market players in the ICT sector to license interoperability information", Brussels, 6.6.2013, SWD(2013)209 fin., p. 12.

117 See *Schweyer*, Die rechtliche Bewertung des Reverse Engineering in Deutschland und den USA, 2012, S. 172 ff.

118 *Behera/Bhaskari*, Procedia Computer Science 2015, 757, 758; *Schweyer*, Die rechtliche Bewertung des Reverse Engineering in Deutschland und den USA, (Diss. 2012), S. 177, 239.

119 See *Behera/Bhaskari*, Procedia Computer Science 2015, 757, 758.

120 See, however, *Schweyer*, Die rechtliche Bewertung des Reverse Engineering in Deutschland und den USA, (Diss. 2012), S. 239-240, arguing in favour of a prohibition of the circumvention of Art. 6 of the Software Directive.

121 Wiebe, Interoperabilität von Software, Jipitec 2011, p. 89, 92. See also: Commission Staff Working Document: "Analysis of measures that could lead significant market players in the ICT sector to license interoperability information", Brussels, 6.6.2013, SWD(2013)209 fin., p. 19. For a comparison with the US approach see John Abbot, Reverse Engineering Software: Copyright and Interoperability, Journal of Law and Information Science 14 (2003), pp. 7 et seq.

122 Commission Staff Working Document: "Analysis of measures that could lead significant market players in the ICT sector to license interoperability information", Brussels, 6.6.2013, SWD(2013)209 fin., p. 8-9, 11.

123 Wiebe, Interoperabilität von Software, Jipitec 2011, p. 89, 95.

124 Wiebe, Interoperabilität von Software, Jipitec 2011, p. 89, 92.

G. Conclusions: Towards a prudent pro-interoperability policy in the digital economy

71 Interoperability features prominently in the rhetoric of the Commission's Digital Agenda.[125] Yet, the Commission was right to drop the idea of imposing a general duty to license interoperability information in the ICT sector within the framework of an Interoperability Directive[126] as temporarily envisaged in 2013.[127]

72 Firstly, interoperability is not – or should not be – an end in itself; it is a means to a broader set of goals: to address market fragmentation; to avoid market tipping towards monopoly; to open downstream markets for competition where the upstream market is monopolized; to increase follow-on innovation irrespective of market power; or to address a perceived societal need for general interconnectedness and communication across competing networks. In each case, before taking action a clear and strong market failure or public service rationale should be identified.

73 Secondly, even if some sort of market failure has been identified, there is no general single best way towards achieving interoperability. The importance of interoperability, its optimal degree, and the optimal path will differ depending on the technological context and the market environment. Due to the complex trade-offs, interoperability issues and potential policy solutions must be analyzed with a view to the relevant sector and technology.

74 Both when applying competition law rules and when considering further-reaching public policy interventions, the existence of different paths to interoperability and the trade-offs inherent in each one of them should be kept in mind. In certain settings, mandated interoperability may still be justified. However the "essential facilities" doctrine in its current form lacks clear boundaries when applied to interoperability problems. Before considering mandated interoperability, it must be established, with some certainty that market solutions ranging from competition for a standard to unilateral or collective standard-setting to adapter or converter solutions will fail. The positive imposition of interoperability requirements must remain a measure of last resort. Although we cannot be sure that the market is always capable of finding the best or even satisfactory solutions for interoperability problems, competition in the market provides the innovating firms with incentives for developing products and services with a degree of interoperability that matches the preferences of consumers. Business strategies that restrict interoperability may be justified by legitimate business concerns. In the midst of a disruptive technological and economic revolution like the digitization of the economy, uncertainty about the appropriate standards and other interoperability solutions calls for caution in imposing top-down public policy solutions. There is a real danger of regulatory failure, and the implementation of wrong solutions may distort and impede technological and economic progress.

75 There is, therefore, a good cause for looking carefully for prudent pro-interoperability policies. In view of the potential cost of mandated interoperability with regard to the path of innovation, a strict proportionality principle should apply. Before mandating access, policy makers, regulatory and competition authorities should strive to support decentralized bottom-up interoperability solutions wherever possible. The EU Commission has started to look for such strategies: user rights to portability of content and/or data may significantly reduce switching cost in a non-interoperable environment. Also, more attention should be given to defining the preconditions under which the pro-active unilateral obstruction of a decentralized search for adapters or converters by a dominant firm may constitute an abuse.

125 Commission, Communication – A Digital Agenda for Europe, COM(2010)245 fin., p. 15: "Since not all pervasive technologies are based on standards, the benefits of interoperability risk being lost in such areas".

126 For this idea see Commission Staff Working Document: "Analysis of measures that could lead significant market players in the ICT sector to license interoperability information", Brussels, 6.6.2013, SWD(2013)209 fin. See also Kroes, How to get more interoperability in Europe, 10 June 2010: "complex antitrust investigations followed by court proceedings are perhaps not the only way to increase interoperability".

127 The idea was dropped for various reasons. The Commission was in doubt whether Art. 114 would provide a sound legal basis. It was also unconvinced that such a regime would be in conformity with the principle of proportionality (Art. 5(4) TFEU). Finally, it was concerned with the need to establish new regulatory institutions in the Member States that would need "to carry out an ex ante analysis of the market for identifying players with significant market power. Moreover, there would be serious technical difficulties to define market power. The analogy with the Access Directive breaks down due to the lack of identifiable market bottleneck assets in software that are equivalent to telecommunications networks". Commission Staff Working Document: "Analysis of measures that could lead significant market players in the ICT sector to license interoperability information", Brussels, 6.6.2013, SWD(2013)209 fin., p. 14-15.

Data Portability - A Tale of Two Concepts

by **Ruth Janal**, Professor of Law at Freie Universität Berlin. In her research, she addresses the interface between Intellectual Property and IT law as well as European Civil Procedure and EU Consumer Law.
Contact: rjanal@zedat.fu-berlin.de. Transcript of a presentation given at the Conference on Digital Goods and Services in Berlin on 6 October 2016.

Abstract: Art. 20 of the General Data Protection Regulation (GDPR) introduces a new concept to European data protection law – the right to data portability. The rule seeks to empower the consumer, to foster the inter-operability of data, and to prevent lock-in effects on closed platforms. Upon request, data controllers are required to provide personal data to the data subject in a structured, commonly used and machine-readable format, which enables the data subject to transfer their personal data between controllers. However, Art. 20 GDPR leaves much room for interpretation, in particular with respect to the data covered, the scope of the exceptions and the requirement of inter-operability. The proposed Directive on certain aspects concerning contracts for the supply of digital content (DCD-proposal) takes matters a step further. Under the DCD-proposal, the supplier of digital content shall provide the consumer with technical means to retrieve all content provided by the consumer (not only personal data) and any other data produced or generated through the consumer's use of the digital content. At the same time, the proposed provisions are stricter than Art. 20 GDPR: The data portability right under Art. 20 GDPR may be exercised at any point in time, whereas the right to content portability under the DCD-proposal only arises after the contract has been terminated following a rule in said directive. The paper highlights other circumstances which warrant a right to content portability and laments the lack of an exception to safeguard the rights and interest of third parties. Three case studies are included to illustrate how the portability rules in the GDPR and the proposed Digital Content Directive might work in practice. The paper closes with a synopsis showing the commonalities and differences of Art. 20 GDPR and the portability rules in the proposed Digital Content Directive.

Keywords: Data portability; portability of content; personal data; EU Privacy Law; EU-GDPR; commonly used data format; contract for the supply of digital content; data as a counter-performance

Recommended citation: Ruth Janal, Data Portability - A Tale of Two Concepts, 8 (2017) JIPITEC 59 para 1.

A. Portability is en vogue

1 Portability of data and content is currently a hot topic in EU law. A right to *data* portability is provided for in Art. 20 of the new *General Data Protection Regulation* (GDPR).[1] The proposed *Directive on certain aspects concerning contracts for the supply of digital* content (DCD-proposal)[2] contains a similar idea with respect to digital *content*. Furthermore, the European Commission has published a *Proposal for a regulation on cross border portability of online content services.*[3]

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1 of 4.5.2016.

2 Art. 13 (2) (c) and Art. 16 (4) (b) of the Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM (2015) 634 of 9.12.2015.

3 Proposal for a Regulation of the European Parliament and of the Council on ensuring the cross-border portability of online content services in the internal market, COM (2015)

These three examples prove that portability is a multi-faceted concept: In the context of Art. 20 GDPR and the DCD-proposal, the term portability describes the right to retrieve data relating to a natural person. In contrast, the proposed rules on cross-border portability seek to ensure that digital content that a consumer has acquired in one Member State can be accessed without fee from any other Member State. While the latter is undoubtedly an interesting subject, this paper focuses on the right to retrieve data and will not address cross-border portability.

2 First, let us take a closer look at the rules which are the subject of this paper. Under Art. 20 GDPR, the data subject shall have the right to receive the personal data concerning themselves, which they have provided to a controller, in a structured, commonly used and machine-readable format and shall have the right to transmit this data to another controller without hindrance. In a similar vein, Art. 13 (2) (c) and Art. 16 (4) (b) of the proposal for a Directive on digital content rule that after the termination of a contract, "the supplier shall provide the consumer with technical means to retrieve all content provided by the consumer and any other data produced or generated through the consumer's use of the digital content." Retrieval shall be possible without significant inconvenience, in reasonable time, and in a commonly used data format.

3 An example of how data and content portability may be put into practice is the Google archive function, which allows Google users to download an archive of their activities regarding most of Google's services simply by selecting the respective service and clicking on a link.[4]

B. Purpose of the portability rules

4 What is the purpose of those provisions? Having considered the matter for quite a while, I cannot supply a definite answer to that question. What I will do is provide an educated guess. It seems that the purpose of Art. 20 Data Protection Regulation is the empowerment of the data subject.[5] To avoid lock-in effects, the data subject shall be empowered to take her personal data from one service and simply move on to another or an additional[6] service. A true relocation naturally only works if the new service is willing to insert the personal data into its own databases.[7] If you want to transfer from Facebook to Google Plus, Art. 20 will only give you a right against Facebook to retrieve your data, but will not give you a remedy to force Google to make use of the data. There is an obvious reason for this: Due to different data formats and different database structures, it can be quite difficult for data controllers to incorporate data provided by another controller. By accepting this limitation, the EU legislator has stopped short of establishing true data empowerment. Thus, it would seem that Art. 20 Data Protection Regulation double-functions as a competition rule.[8] If a company is interested in winning customers from another service, Art. 20 will improve competition on the market, because a competitor can promise its potential customers to integrate their personal data (or parts thereof), if they bring their data with them. One prominent example would be social networks that incorporate their users' contacts via the email provider's contact API.[9]

5 The purpose of Art. 13 (2)(c) and Art. 16(4)(b) of the Digital Content Proposal is more straightforward. Under the proposed directive, the right to portability only arises after the contract has been terminated by the consumer. Imagine you are a member of a particular platform and you have provided quite a bit of content – pictures, comments, and so forth. Then something happens that makes you want to terminate the contract. Obviously, the fear that your content may be lost if you terminate the agreement will play a role in the decision of whether to exercise your rights. Thus, the data portability rules of the Digital Content Proposal safeguard the consumer's right of termination in order to avoid lock-in effects.[10] The fostering of competition is a

627 of 9.12.2015.

4 <https://takeout.google.com/settings/takeout>.

5 According to recital 68 GDRP, data portability strengthens the data subject's control over his or her own data; see also *Article 29 Data Protection Working Party*, Guidelines on the right to data portability, 13.12.2016, 16/EN WP 242, p. 4; *Maisch*, Informationelle Selbstbestimmung in Netzwerken, Berlin 2015, p. 311.

6 The simultaneous presence on multiple similar or equivalent platforms is referred to as "multi-homing".

7 *Kühling/Martini*, EuZW 2016, 448 (450).

8 *Article 29 Working Party* (fn. 4), p. 4. Commission Staff Working Document on the free flow of data and emerging issues of the European data economy of 10.1.2017, SWD (2017) 2, p. 11. In a similar vain see *Härting*, BB 2012, 459 (465); *Kipker/Voskamp*, DuD 2012, 737 (740); *Kühling/Martini*, EuZW 2016, 448 (450); *Schantz*, NJW 2016, 1841 (1845); Antwort der Bundesregierung auf Kleine Anfrage (Drucksache 17/10452), p. 7. For the economic consequences of portability cf. Commission Staff Working Document (ibid), p. 47 et seq.

9 For further examples see *Article 29 Working Party* (fn. 4), p. 5. For the dispute between Facebook and Google regarding the contact API cf. *Singel*, Google Calls Out Facebook's Data Hypocrisy, Blocks Gmail Import, 11.5.2010 <https://www.wired.com/2010/11/google-facebook-data> and *Metz*, Facebook engineer bashes Google for Gmail block – When hypocrisies collide, 10.10.2010 <http://www.theregister.co.uk/2010/11/10/google_v_facebook_contact_fight_round_two>.

10 See also recital 39 of the DCD-proposal; summary of results of the public consultation on contract rules for online purchases of digital content and tangible goods, <http://ec.europa.eu/justice/contract/files/summary_of_results.docx>, p. 2.

welcome side effect.[11] With that in mind, let us now consider under which circumstances a right to data portability arises and what such a right entails.

C. Art. 20 General Data Protection Regulation

I. Prerequisites

6 I shall first take a closer look at Art. 20 GDPR, a rule which will apply as of 25 May 2018. The General Data Protection Regulation applies to the processing of personal data by automated means.[12] What is further required is some connection to the European Union,[13] in the form of a) the controller's establishment within the EU, b) the offer of goods or services to data subjects in the Union, or c) the monitoring of behaviour which occurs within the European Union.

7 When does the portability requirement arise? Art. 20 GDPR requires portability for personal data[14] which the data subject has provided to a controller. Personal data means "any information relating to an identified or identifiable natural person", the so-called "data subject".[15] There is some room for debate as to which data has been "provided" by the data subject. Clearly, the wording of the provision covers personal data explicitly provided by the data subject, such as contact information, comments und uploaded material. However, does it also refer to data which has been provided by the data subject's conduct or use of a gadget or service – perhaps even unwittingly?[16]

8 As an example, consider a sensor which measures the data subject's heart rate. The data is provided quite willingly by an athlete wearing a fitness tracker with a sensor, and when the athlete changes suppliers, she may be interested in transferring that data to another controller. This would allow the athlete to monitor her heart rate over a longer period of time, irrespective of the contractual relationship with a particular supplier. However, take note that an identical sensor may also be incorporated into a car seat. There, it would form part of the attention assist system of the car. By measuring the heart rate, the system can determine signs of fatigue and alert the driver that she should take a break or switch drivers. In this instance, the driver may or may not be aware of the fact that her heart rate is tracked, and she may or may not have consented to that tracking, but in any case she will generally not be interested in keeping a record of that heart rate.

9 Turning back to Art. 20 GDPR, has the heart rate data been "provided" by the athlete and the driver? Arguably, the data was "collected" by the provider, rather than being "provided" by the data subject. However, this take on the matter would not be very convincing. At least in those instances where the collection of the data is based on the data subject's consent, there is an active element of provision by the data subject.[17] This position is supported by recital 60 sent. 4 GDPR, where collection of data is considered a form of provision of data by the data subject.[18] More importantly, if the purpose of Art. 20 GDPR is empowerment and market competition, those goals will only be achieved if the right to portability extends to data provided by the consumer's conduct and use of gadgets or services. The user of a fitness tracker may switch providers more willingly, if she is able to retrieve her fitness data and transfer it to her new provider. This might allow the athlete to compare the fitness data of her last marathon with the data of her current run.

10 That being said, it seems slightly over the top to extend the portability right to each and every data collected by the data controller, as is evidenced by the example of the car's attention alert system. For this reason, it is a pity that Art. 20 GDPR does

11 Recital 46 DCD-proposal; *Spindler*, MMR 2016, 219 (221 et seq.).

12 Art. 2 (1) GDPR, which furthermore provides that the Directive also applies "to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."

13 Art. 2 (1) GDPR.

14 Regarding the portability of other data cf. the observations in the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 10.1.2017, COM (2017) 9, "Building a European Data Economy", p. 15 et seq.

15 The definition provided in Art. 4(1) GDPR explains that "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". Recital 26 further explains that a person is deemed identifiably if she can be identified by the controller or another person using reasonable means.

16 In the affirmative *Maisch*, Informationelle Selbstbestimmung in Netzwerken, Berlin 2015, p. 304; *Spindler*, MMR 2016, 219 (222); in the negative submission of the Handelsverband Deutschland e.V. (HDE) (1), <http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/AbteilungenReferate/IB6_VA_Digitales_Vertragsrecht_Stellungnahme_HDE_2.pdf>, p. 2.

17 Cf. *Article 29 Working Party* (fn. 4), p. 8: "Observed data are 'provided' by the data subject by virtue of the use of the service or the device". The Commission Staff Working Document on the free flow of data and emerging issues of the European data economy of 10.1.2017, SWD (2017) 2, p. 46, seems to share this view.

18 "Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data."

not contain a reasonability or proportionality restriction.[19] One option would be to simply read a proportionality requirement into the rule. For example, a right to data portability should only arise where there is a reasonable expectation on the part of the data subject that the data will be available over time. However, I will readily admit that the wording of Art. 20 GDPR does not lend itself to this distinction. Rather, the text relates to *any* data that has been provided by the data subject and is still retained by the controller.

11 Finally, the right to data portability under Art. 20 (1) GDPR only arises where the processing of data is carried out by automated means and where it is either based on the data subject's consent or the processing is necessary for the performance of a contract. This wording is too restrictive because it does not cover situations where the controller has illegally processed the data. The point of Art. 20(1) (a) GDPR is to relieve a controller from the portability requirement if the processing of data is based on the legal grounds of Art. 6 (1) (c) to (f) and Art. 9 (2) (b) to (j) GDPR.[20] The portability right should however apply if a controller has illegally processed the data as there is no conceivable reason to reward the contravention by excluding the data subject's right to retrieve data.

II. Exceptions

12 Art. 20 GDPR specifies three exceptions to the right to retrieve data. Firstly, the right only applies to data still retained by the controller – certainly if the data subject exercises her right to be forgotten under Art. 17 GDPR, she cannot simultaneously retrieve the data. The same is true for data that has been rendered anonymous and no longer pertains to an identifiable person.[21] Secondly, the portability right may not interfere with a task carried out in the public interest.[22] Thirdly, portability shall not adversely affect the rights and freedoms of others.

13 Considering the third exception in particular, personal data will oftentimes relate to more than one data subject: a picture may show more than one person; a work may be a collaborative effort; and communication by its very meaning requires at least one originator and one addressee. When does the retrieval by the data subject interfere with the rights and freedoms of another data subject? One approach is to allow data portability only if, under the new controller, the data is kept under the sole control of the requesting user and the data is managed for purely personal or household needs.[23] I believe this approach may prove to be too strict. Namely, when the data subject requesting portability provided this data to the original controller, the other data subjects may not have been asked for their consent. Imagine a list of contacts provided by one data subject to a controller; when this list is ported to another controller, why should only the original controller be entitled to process the data under Art. 6 (1) (f) GDPR, but not the controller whom the data was ported to?

14 Alternatively therefore, I propose to answer the question by looking at the reasonable expectation of the other data subject involved. For example, if there is a group discussion on a social media platform, the expectation will generally be that views are exchanged on this platform and on this platform only. The group members cannot individually exercise their right to data portability, while mutual consent would allow them to exercise their rights collectively. In contrast, if someone converses via email, there is generally no reasonable expectation that the communication will be stored with a specific email provider. Thus, the rights and freedoms of the participant of an email exchange will not stand in the way of portability.

III. Consequences

15 Once the data subject has established the right to retrieve data, the obvious question is, what does the right entail? Under Art. 20 GDPR, the data subject has a right to receive the data in a structured, commonly used and machine-readable format (within one month of the receipt of the request – Art. 12(3) GDPR). The wording implies that it is not sufficient if the data subject can manually extract individual data. Rather, the controller has to provide a structured set of data. Where technically feasible, the data subject may require the controller to transmit that data directly to another controller. Both reception and transmission can be required at any point in time and are in principal free of charge.[24]

19 Cf. *Werkmeister/Brandt*, CR 2016, 233 (237).

20 Recital 68 GDPR states: "That right [to retrieve data] should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract."

21 Cf. recital 26 GDPR; *Article 29 Working Party* (fn. 4), p. 7.

22 On the concept of public interest cf. recital 73 GDPR.

23 *Article 29 Working Party* (fn. 4), p. 10.

24 Art. 12 (5) GDPR; this does not apply to manifestly unfounded or excessive (i.e. repetitive) requests. *Article 29 Working Party* (fn. 4), p. 12 argues that "For information society or similar online services that specialise in automated processing of personal data, it is very unlikely that the answering of multiple data portability requests should generally be considered to impose an excessive burden".

16 The rule implies that there are commonly used data formats for all kinds of data. While this may be true for a lot of data, it is certainly not true for all kinds of data – consider the "likes" on a social media platform, or the data of a particular seat or mirror position in a car. What can be done if a commonly used data format simply does not exist? Must Art. 20 GDPR be understood as an impetus to develop such commonly used data formats? I would rather argue that in such an instance, the controller may fulfil the portability requirement by providing the data in the format presently used. It is also unclear how the standard of technical feasibility of a direct transfer of data is to be determined. Something which is technically feasible for companies such as Facebook and Google, may be difficult to implement for smaller controllers that have to rely on software developed and supported by third parties.[25]

IV. Enforcement

17 Before I turn to some examples, I should briefly note that the enforcement mechanism of the General Data Protection Regulation is two-fold: The failure to ensure data portability may lead to civil liability and a right to compensation under Art. 82 GDPR. Possibly of higher importance are the administrative powers of the supervisory authority, which include the imposition of fines of up to 20.000.000 EUR, or up to 4 % of the total worldwide annual turnover, Art. 58, 83 (1), (5) GDPR.

V. Examples

18 It has been reported that the primary aim of Art. 20 GDPR was to avoid lock-in effects in social media networks.[26] Needless to say, the rule has a much broader scope and covers many industries distinct from social media. Below are a few examples.

1. Student vs. University

19 Suppose a student wishes to transfer from one university to another. The student asks her current university to transmit all personal data to the new school. Personal data stored by the university will likely encompass registration data, academic transcript information, the emails stored by the university mail provider, and any learning platform data, such as tests, discussion board posts etc.

20 Four aspects warrant consideration. First, was the processing of this data necessary for the performance of a task carried out in the public interest or in the exercise of official authority – in which case the exception in Art. 20(3) GDPR would apply? Even with respect to public learning institutions, I do not believe that this exception is intended to cover universities (a distinction between private and public learning institutions would hardly make sense with respect to portability). Secondly, which of this data has been provided by the student? Certainly grades are provided by members of the university staff, and emails that a student has *received* have been provided by their originator. A right to portability would therefore not arise with respect to this data. Third, is it technically feasible to transfer the data from one institution from the other? Oftentimes, universities rely on databases developed by third parties. Should the standard of feasibility be determined from the perspective of the universities involved or from the perspective of the respective software developers? Finally, the online quizzes a student has taken have been developed by lecturers and chats on the learning platform may involve a multitude of students. With respect to this information, the rights and freedom of third parties interfere with the student's right to portability. If we follow the standard proposed above (C.II.), this information cannot be transferred to another controller, because the parties involved had a reasonable expectation that the information was platform-specific and would stay on the learning platform.

21 The – somewhat surprising – conclusion is that most of the data retained by the university is not covered by the student's portability right. In particular, while the student will probably be mostly interested in transferring transcript data and emails received to the new university, portability is not guaranteed with respect to this information. This result seems acceptable if Art. 20 GDPR is solely viewed as a competition rule, because lock-in effects on the market for education seem unlikely. If the purpose of the rule is data empowerment, then the rule fails to achieve its aim in our example.

2. Car owner vs. Manufacturer

22 We all know that with the arrival of automated driving, our cars will resemble computers with wheels rather than machines with embedded software. In terms of data collected by car manufacturers, the days of connected driving have

25 Regarding the potential use of personal information management services see Commission Staff Working Document on the free flow of data and emerging issues of the European data economy of 10.1.2017, SWD (2017) 2, p. 11.

26 *Härting*, BB 2012, 459 (465); *Kipker/Voskamp*, DuD 2012, 737 (740).

already arrived. A recent investigation of ADAC, the German automobile club, has offered some insight into data collected by German manufacturers.[27] Here is a list of some of the data which is collected and periodically transmitted to the manufacturer: the position of the car; the number of electromotive seat-belt tensions; engine speed and temperature; operating hours of the lights; number of seat adjustments; status report on windows; selected program of the automatic transmission; miles travelled on motorways, country roads and city streets. Furthermore, modern cars provide the option of saving individual driver preferences (seat and mirror position, temperature, language used to communicate with the board terminal etc.), often accessed by means of biometric information, such as the driver's fingerprint or voice. The majority of this data is personal, because a connection with an individual data subject (car owner or driver) may be established by various means.

23 If we consider the data as "provided" by the data subject (see above at C.I.), which should be the case at least regarding information actively saved by a particular driver (personal preferences as to seat, mirror, temperature), then a right to data portability arises. Is there a structured, commonly used format in which the data could be transmitted? This is so-far unclear. From the evidence available, each manufacturer uses its own proprietary data format, with few common standards. Then again, some data may at least be stored in a similar format (i.e. the data recorded in the car's event data recorder),[28] which brings us the question raised above of whether there is an obligation on controllers to develop a standard format.

3. User vs. online marketplace

24 Finally, let us take a look at online marketplaces such as *eBay* and *Amazon Marketplace*. These platforms process a multitude of data, such as registration data, transaction data, social data (ratings, personal messages, discussion board postings), user-generated data (search history, wish lists, preferences, gadgets used, IP addresses, information revealed by cookies etc.). Most, but not all of this data will be personal. In particular, some of the transaction-based data may simply be goods-related, such as the description of an item offered for sale. Again, the big question is which of this data has been *provided* by the data subject and is subject to the portability requirement.

27 <https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/daten_im_auto/default.aspx?ComponentId=260789&SourcePageId=227535>.

28 Cf. minimum data elements required for all vehicles equipped with an event data recorder, <http://www.crashdatagroup.com/learnmore/howitworks.html>.

What seems to be clear is that the right to data portability does not encompass two important sets of data. (1) User profiles (patterns, preferences, scores) are established by the platform provider and not provided by the data subject;[29] thus Art. 20 GDPR does not require the platform provider to release this valuable know-how. (2) The portability right also does not extend to online ratings, because the information contained in online rating systems is provided by *other* users of the system, not by the data subject herself.

VI. Takeaways regarding Art. 20 GDPR

25 There are two main takeaways from this quick look at Art. 20 GDPR. First, there remains some food for thought on the interpretation of that rule until 25 May 2018 (which is the day on which the GDPR will start to apply). Second, the scope of the rules and therefore its positive effect on competition has some limitations, as it only extends to personal data provided by the data subject. Bearing that in mind, let us examine whether help is under way in form of the portability rules in the DCD-proposal.

D. Data and Content Portability in the Proposal for a Digital Content Directive

26 The proposal for a *Directive on certain aspects concerning contracts for the supply of digital content* contains two provisions on portability. The proposed rules differ from Art. 20 GDPR in two important aspects: (1) they only apply after the termination of a B2C-contract for the supply of digital content and; (2) the right to portability is not limited to personal data, but extends to all kinds of digital content.

I. Contracts covered by the Proposal

27 A lot of ink has already been spilled on the kinds of contracts covered by the proposed Directive,[30]

29 *Article 29 Working Party* (fn. 4), p. 8.

30 *Bokor*, Die Richtlinienvorschläge der Kommission zu Verträgen über digitalen Inhalt und Online-Warenhandel, p. 4 et seq.; submission of the Bundesverband Interaktive Unterhaltungssoftware e.V. (BIU), <http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/AbteilungenReferate/IB6_VA_Digitales_Vertragsrecht_Stellungnahme_BIU.pdf>, p. 2; submission of the TRUSTED SHOPS GmbH, <http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/AbteilungenReferate/IB6_VA_Digitales_Vertragsrecht_Stellungnahme_Trusted_Shops_AG.pdf>, p. 3.

thus I shall keep my comments brief in that regard. The Directive shall apply to business-to-consumer-contracts for the supply of digital content, such as video and audio files, software, cloud storage, social media and visual modelling files for 3D printing,[31] as well as games, email provision, online marketplaces and sharing platforms.[32] Once those rules have been implemented in the national laws of the Member States, the portability provisions will apply whenever the rules of private international law point to the contract law of an EU Member State (cf. Art. 4 and 6 Rom I-Regulation).

28 The proposed Directive mandates that the contract require the consumer to either pay a price or actively provide counter-performance other than money in the form of data. The prerequisite of an "active" provision of data is both vague[33] and inappropriate from a policy perspective.[34] Namely, data that is collected from the consumer during the performance of a service will often be of more interest to the supplier than data which the consumer has actively volunteered. The intention of the Commission seems to be to exclude contracts that do not require registration.[35] Even where the consumer actively provides personal data, this data shall not be considered a counter-performance if the data is strictly necessary for the performance of the contract or for meeting legal requirements, as long as the supplier does not make use of the data for other purposes, in particular commercial ones.[36] Consequently, there may be instances in which the provision of data is not considered an active counter-performance. However, in practice this exemption will rarely come into play because consumer data is regularly used by suppliers for other purposes than the performance of the contract.

29 The requirement of "active" provision of data is also of interest with respect to embedded software, a problematic issue in its own right. According to recital 11 of the DCD-proposal and recital 13 of the proposed Directive on the online sales of goods,[37] the proposed Online Sales Directive shall apply to embedded software if the software's functions are subordinate to the main functionalities of the goods and it operates as an integral part of the goods. This distinction has been widely criticized.[38] With respect to data portability, the crux of the matter is a particular one: Bear in mind that the seller of the good or supplier of the embedded software and the person collecting data by means of the embedded software will often be different parties. When a fitness tracker, a smartphone, or a car is

31 Explanatory Memorandum DCD-proposal, p. 11.

32 *Spindler*, Stellungnahme zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragliche Aspekte der Bereitstellung digitaler Inhalte, <https://www.bundestag.de/blob/420320/f592286ecb85f113710d7bd40bd92b47/spindler-data.pdf>, p. 5; *Wendland*, GPR 2016, 8 (12).

33 Recital 14 sheds some light as to what is meant by an „active" provision of data: registration by the consumer is seen as actively providing data, accepting a cookie is not.

34 Cf. also *Schmidt-Kessel*, Präsentation: Daten als Gegenleistung in Verträgen über die Bereitstellung digitaler Inhalte, 03.05.2015, <http://www.bmjv.de/SharedDocs/Downloads/DE/Praesentationen/05032016_digitalesVertragsrecht_Schmidt_Kessler.pdf>, p. 17; *Wendehorst*, Präsentation: Gewährleistung für digitale Inhalte im Lichte des Richtlinienentwurfs COM(2015) 634, 03.05.2016, <http://www.bmjv.de/SharedDocs/Downloads/DE/Praesentationen/05032016_digitalesVertragsrecht_Wendehorst.pdf>, p. 7; *v.Westphalen*, Stellungnahme zum Entwurf der Richtlinie 2015/634, <https://www.bmjv.de/SharedDocs/Downloads/DE/PDF/AbteilungenReferate/IB6_VA_Digitales_Vertragsrecht_Stellungnahme_RA_Graf_v_Westphalen.pdf>, p. 1; submission of the Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. (vzbz), <http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/AbteilungenReferate/IB6_VA_Digitales_Vertragsrecht_Stellungnahme_VZBV.pdf>, p. 7.

35 *Spindler*, Stellungnahme zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragliche Aspekte der Bereitstellung digitaler Inhalte, <https://www.bundestag.de/blob/420320/f592286ecb85f113710d7bd40bd92b47/spindler-data.pdf>, p. 8.

36 Cf. Art. 3(5) DCD-Proposal. Processing with a purpose which is not contract-related will thus retroactively lead to the application of the proposed Directive, cf. the critical assessment of *Stürner*, Stellungnahme zu den Kommissionsvorschlägen COM(2015) 634 und COM(2015) 635, 04.05.2016, <https://www.bundestag.de/blob/422106/efd7cdf67eb00e2c82d577d7c480bcfb/stuerner-data.pdf>, p. 12 et seq.

37 Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods, COM(2015) 635 of 9.12.2015.

38 Submission of the Bundesverband der Deutschen Industrie e.V. (BDI), <http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/AbteilungenReferate/IB6_VA_Digitales_Vertragsrecht_Stellungnahme_BDI.pdf>, p. 4; submission of the Bundesverband E-Commerce und Versandhandel Deutschlande.V.(bevh),<http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/AbteilungenReferate/IB6_VA_Digitales_Vertragsrecht_Stellungnahme_bevh.pdf>, p.3; submission of the Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) (2), <http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/AbteilungenReferate/IB6_VA_Digitales_Vertragsrecht_Stellungnahme_Bitkom_2.pdf>, p. 5 et seq.; submission of the Bundesverband Interaktive Unterhaltungssoftware e.V. (BIU), <http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/AbteilungenReferate/IB6_VA_Digitales_Vertragsrecht_Stellungnahme_BIU.pdf>, p. 5; submission of the Verbraucherzentrale Bundesverband e.V. (vzbv), <http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/AbteilungenReferate/IB6_VA_Digitales_Vertragsrecht_Stellungnahme_VZBV.pdf>, p. 4, 8; submission of the Zentralverband Elektrotechnik- und Elektroindustrie e.V. (ZVEI), <http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/AbteilungenReferate/IB6_VA_Digitales_Vertragsrecht_Stellungnahme_ZVEI.pdf>, p. 4.

sold, the contract is between seller and consumer; thus the seller would be obliged to return data and digital content to the consumer. However, the seller does not usually collect the data generated through the use of embedded software. Typically, the consumer's data is collected instead by the producer of the gadget or of the gadget's operating system. A right to retrieve data and content from the producer however, will only arise if consumer and producer have formed a separate contract for the provision of digital content in the meaning of Art. 3 DCD-proposal. It seems worthwhile to keep this tripartite relationship in mind when devising the application sphere of the final DCD- and Online Sales Regulations.

II. Termination of contract

30 Let us assume the relationship between consumer and supplier satisfies the requirements of Art. 3 DCD-proposal. After clearing this first hurdle, we find ourselves immediately facing a second obstacle; namely, the consumer's right to retrieve data and content arises only if the consumer has exercised her right to terminate the contract according to a provision of the DCD-Proposal. This approach is unconvincing because the proposed directive addresses only a small segment of possible grounds for termination. Art. 12 (5) DCD-proposal allows the consumer to terminate the contract for lack of conformity, and Art. 16 (1) DCD-proposal gives the consumer the right to terminate a long-term contract any time after the expiration of the first 12-month period.

31 Obviously, there are several other reasons why a B2C-contract may be terminated: the exercise of a right of withdrawal under Art. 9 Consumer Rights Directive;[39] a contractually stipulated right of termination before the end of a 12 month-period; or a contract with a shorter duration than 12 months. In the case of embedded software, the consumer might rescind the contract with the seller because the good is defective,[40] and might consequently no longer be interested in the contract with the supplier of the digital content. If portability is to safeguard the consumer's right to sever ties with the supplier and to avoid lock-in effects, then the right to retrieve data should also exist in those instances.

III. Exceptions

32 The right to retrieve data and content arises once the consumer exercises her right to terminate the contract under Art. 12 (5) or Art. 16 (1) DCD-Proposal. It encompasses any content provided by the consumer and any other data produced or generated through the consumer's use of the digital content. The proposal clarifies that the supplier is not required to retain any data in order to allow for portability.[41] Likewise, if the supplier has taken successful measures to anonymize the data, he should not be considered to have retained the data.[42]

33 Strikingly, there is no exemption for the rights and freedoms of third parties, even though the supplier obviously has to safeguard other parties' data protection rights. This is a clear gap which should be closed along the lines suggested above regarding Art. 20 (4) GDPR (III.2.). If no amends are made, the supplier might be caught between a rock (portability right of the consumer) and a hard place (data protection of the other natural persons involved).

34 Another aspect which needs to be addressed is the requirement of proportionality. In line with Art. 20 GDPR, the portability rules of the proposed directive currently do not contain a reasonability restriction. As the scope of the portability right under the DCD-proposal entails not only personal data, but also user-generated content, such a restriction is sorely missed. This can be illustrated by looking at the gaming industry – exporting an avatar created by a gamer into a different game is virtually impossible and generally not of interest to the consumer.[43] In this context, the provision of a portability right seems unreasonable and disproportionate.

39 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, OJ L 304/64 of 22.11.2011; the exception in Art. 16 m Consumer Rights Directive does not cover all of the contracts within the scope of the DCD-proposal.

40 Cf. Art. 3 (5) Consumer Sales Directive / Art. 9 (3) Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods, COM(2015) 635 final of 09.12.2015.

41 Recital 39 DCD-proposal clarifies that the obligation extends to any data which the supplier has effectively retained in relation to the contract.

42 *Spindler*, MMR 2016, 219 (222); Submission of the Handelsverband Deutschland e.V. (HDE) (1), <http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/AbteilungenReferate/IB6_VA_Digitales_Vertragsrecht_Stellungnahme_HDE_1.pdf>, p. 12.

43 Submission of the Bundesverband Interaktive Unterhaltungssoftware e.V. (BIU), <http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/AbteilungenReferate/IB6_VA_Digitales_Vertragsrecht_Stellungnahme_BIU.pdf>, p. 12 et seq.

IV. Consequences

35 As I have already noted, the implications of Art. 13 (2)(c) and Art. 16(4)(b) DCD-Proposal are much broader than those of Art. 20 GDPR. Portability is not only required with respect to personal data,[44] but also with respect to any other content provided by the consumer and any data produced or generated through the consumer's use of the digital content. This would apply i.e. to pictures uploaded by the consumer, as well as to a photo book which the consumer has created online.

36 How is portability to be achieved? In that respect, the DCD-proposal is more lenient than Art. 20 GDPR. The supplier shall provide the consumer with the technical means to retrieve the content, without significant inconvenience, in reasonable time and in a commonly used data format. As there is no requirement to provide the data in a structured format, suppliers may seemingly refer their customers to extract the material manually/individually, as long as this does not cause significant inconvenience. The data is to be provided in a commonly used data format, which would give the supplier a choice from various formats on the market. Again, there is no indication on how to proceed when a common data format is non-existent. Note that – unlike Art. 20 GDPR – the DCD-proposal does not include a right to have the content transferred from one supplier to another.

37 Under the current proposal, portability is free of charge only if requested after the consumer terminates the contract due to a lack of conformity, whereas the supplier is entitled to demand a fee in the context of Art. 16 (4)(b) DCD-proposal.[45] I find this distinction misguided. First of all, the consumer is entitled to retrieve some of this data free of charge due to Art. 20 GDPR and allowing for a fee in the context of Art. 16 (4)(b) DCD-proposal might obscure that right. Secondly, if the aim of portability in the context of the DCD-proposal is to safeguard the consumer's right to terminate the contract, that aim will not be achieved if the consumer is required to pay a fee to retrieve the content. Finally, any fee requested by the supplier would have to be adequate to avoid a deterrent effect on the consumer, and satellite litigation regarding the adequacy of the fee might ensue.

44 *Spindler*, MMR 2016, 219, 222: It is uncertain, whether the „other data" also includes all personal data. Considering the broad interpretation of the term, it includes both personal data and user-generated content, even if the data is produced by the supplier.

45 Argumentum a contrario Art. 13 (2) (c), cf. also recital 40.

V. Enforcement

38 The issue of enforcement of the portability rules in the DCD-proposal is left to the Member States. Art. 18 DCD-proposal contains the typical requirement that Member States shall implement adequate and effective means to ensure compliance and must provide for representative actions.

VI. Examples

39 I will now return to the previous examples to illustrate the workings of Art. 13(2)(c) and 16(4)(b) DCD-proposal.

1. Student vs. university

40 In the case of a student requesting data from the university, the first question is whether a contract for the supply of digital content exists between the student and her university. Evidently the relationship between student and university has a much broader ambit, but services such as campus management, learning platforms and email provision are certainly digital content within the meaning of the proposed directive. Following Art. 3(6) DCD-proposal, the directive shall apply to the obligations and remedies of the parties as supplier and consumer of the digital content, even if a contract includes elements in addition to the supply of digital content. Within a university context however, education is not an addition to the digital services. Rather, the digital services are offered as additions to the provision of education as the university's main obligation.

2. Car owner vs. manufacturer

41 In the case of the car owner, assume that the owner has bought a BMW 320d which is defective. She would like to terminate the contract and instead buy a Mercedes B-class, which – as an investigation by the ADAC has shown – collects more or less the same data as the BMW.[46] The termination of the contract with the seller will follow the rules of the Consumer Sales Directive or the proposed Online Sales Directive. Neither of those directives provide for data portability. Is there a separate contract for the supply of digital content with a corresponding counter-performance by the car owner, which might trigger a right to portability? Generally speaking

46 Cf. <https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/daten_im_auto/default.aspx?ComponentId=260789&SourcePageId=227535>.

there is not. However, if the owner has registered with *BMW connected drive* or the equivalent *Mercedes me*-Service, the relationship between owner and manufacturer will meet the requirements of a contract for the supply of digital content. Even in that case, the consumer will not have a right to data portability, since the contract was not terminated under Art. 12(5) or Art. 16 (1) DCD-proposal. Consequently, the car owner or driver would have to rely on Art. 20 GDPR to realize portability.

3. User vs. online marketplace

42 Our last example pertains to online marketplaces such as *eBay* and *Amazon Marketplace*. Do these platforms provide digital content? Following Art. 2 (1)(b) of the DCD-proposal, the definition of "digital content" includes services allowing the creation, processing and storage of data in a digital form, where that data is provided by the consumer. Thus, if a consumer is using the platform to sell a good, the user agreement will be covered by the DCD-proposal. What if the consumer is using the platform to buy a product? In this instance, Art. 2 (1)(c) comes into play, according to which digital content also encompasses "a service allowing sharing of and any other interaction with data in digital form provided by other users of the service". Does the consumer offer a counter-performance? Obviously, that depends on the platform model. Usually the registration as such and the purchase of goods on the platform is without charge, while a fee may be requested if the consumer sells something via the platform. Even if the supplier does not charge a fee, the contract will usually fall within the application sphere of the DCD-proposal because the consumer actively provides counter-performance in the form of data and this data is usually put to some commercial use (thus rendering the exception in Art. 3 (4) DCD-proposal inapplicable).

43 As mentioned above (III.5.c.), data portability under Art. 20 GDPR only relates to *personal data* and thus may not cover transaction-related data. In contrast, the portability rules of the DCD-proposal apply to *all content* provided by the consumer, which includes non-personal pictures or the description of a good sold. Furthermore, the proposal is clear that the right to retrieve data also applies to data produced or generated through the consumer's use of the digital content (to the extent that data has been retained by the supplier). Under the current wording, the portability right even extends to user profiles (patterns, preferences, scores) established by the supplier. While I do not believe that the Commission intends to require businesses to reveal such sensitive know how, a clarification of this matter would be welcome.[47] Furthermore, recital 15 DCD-proposal suggests that online ratings are supposed to be portable. Again, this is not immediately clear from the wording of the provisions ("data generated through the consumer's use of the digital content"), since platform users often rate the consumer's performance in the "real world" (conformity of the good sold or the apartment rented), rather than rating her platform conduct. A clarification might be helpful. In any case, bear in mind that the right to retrieve the data only arises if the contract is terminated due to faulty service or after more than 12 months.

E. Relationship between the three portability provisions

44 Having considered these three examples, a final question remains. Namely, what is the relationship between the portability rules addressed in this presentation? There is a clear-cut distinction between Art. 13(2)(c) and Art. 16(4)(b) DCD-proposal: the former applies to the termination of contract for lack of conformity, whereas the latter applies when the contract has been terminated by the consumer after 12 months plus.

45 If a right to portability arises both under Art. 20 GDPR and one of the provisions of the DCD-proposal, the consumer may choose which rule they rely upon – or may even rely upon both. Art. 3 (8) DCD-proposal clarifies that the rules of the DCD-proposal are without prejudice to data protection rules.[48] It makes sense that neither portability rule takes precedence over the other, as the provisions show both peculiarities and significant overlap. If the consumer's requirements are met by a request under one Directive, the consumer will not have to additionally resort to the other Directive. On the other hand, where some of the consumer's requirements will only be met under Art. 20 GDPR (transmission to another supplier) and other demands will only be met under the DCD-proposal (portability of content other than personal data), it is helpful for the consumer to combine both rights.

47 See also submission of the Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., <https://www.gdd.de/downloads/aktuelles/stellungnahmen/Stellungnahme%20DS-GVO-E%20endgx.pdf>, p. 10.

48 The relationship between GDPR and DCD-proposal is not addressed by Art. 3 (7) DCD-proposal. The provisions are not in conflict with each other, and neither of the two acts is more specific; rather, they address a different subject matter.

F. Closing Remarks

46 Data portability is a hot topic as well as a novel topic. It is therefore hardly surprising that the rules addressed in this article offer some room for improvement. With respect to Art. 20 GDPR, the challenge ahead lies in the development of a lucid interpretation of the rule. Currently, it is unclear which data is deemed to be *provided* by the data subject and which standard should be applied to determine the technical feasibility of transmission.

47 The portability rules in the DCD-proposal will certainly undergo a change before they are enacted. What is needed is a clarification of the application sphere, especially with respect to embedded software. The portability right should arise with the termination of contract, irrespective of the ground for termination. One might even consider a right to retrieve content at any point in time during the performance of the contract. Portability should be free of charge in all instances, barring abusive conduct of the consumer. Finally, there is an urgent need to introduce some exceptions to the rule – the portability provisions of the DCD-provisions should acknowledge the rights and interests of third parties as well as the legitimate interest of the supplier, which includes a limit for reasons of proportionality.

G. Synopsis of commonalities and differences

48 The following synopsis gives an overview of the many commonalities, but also a number of key differences between the portability rules of the GDPR and the DCD-proposal:

	Art. 20 General Data Protection Regulation	Art. 13 (2)(c), 16 (4)(b) proposed Directive on Digital Content
purpose	competition / empowerment	safeguard for right of termination
application sphere	Art. 2 (1) GDPR • processing of personal data wholly or partly by automated means • connecting factor to EU	Art. 3 DCD-Proposal • B2C-contract for the supply of digital content • counter performance: either price or active provision of data • applicable contract law = law of EU member state (Art. 6 Rome I Reg.)
data covered	• personal data provided by data subject	• any content provided by the consumer • any other data produced or generated through the consumer's use of the digital content
prerequisites	• processing based on consent or contract and carried out by automated means • data still retained by controller	• termination for lack of conformity, Art. 13 (2)(c) DCD-proposal • termination after 12 months +, Art. 16(4)(c) DCD-proposal • data / content retained by supplier
exceptions	• task in the public interest or in the exercise of official authority • rights and freedoms of others	• no explicit exceptions
point in time	anytime	after termination of contract
consequences	• right to receive the data in a structured, commonly used and machine-readable format • right to transmit data directly from one controller to another, where technically feasible	• technical means to retrieve content and data • without significant inconvenience, in reasonable time and in a commonly used data format
fee	• free of charge (exceptions see Art. 12 (5) GDPR)	• free of charge in case of Art. 13(2 • fee possible in case of Art. 16 (4)
relationship		without prejudice to data protection, Art. 3 (8) DCD-Proposal
enforcement	• compensation, Art. 82 GDPR • administrative fines, Art. 58, 83 (1), (5) GDPR	• adequate and effective means (left to Member States), Art. 18 • representative actions

Is Data Protection Law Growing Teeth?

The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR

by **Sebastian J. Golla**, Dr. iur, research assistant at Johannes Gutenberg-Universität Mainz*

Abstract: This article looks at the current lack of enforcement and sanctions in European Data Protection Law with a particular focus on administrative fines. It identifies reasons for the existing deficits in European Data Protection Law and analyses the potential of the new rules of the General Data Protection Regulation (GDPR) to compensate for those deficits. The article argues that the practical application of the new rules and the coordination of Data Protection Authorities (DPAs) in all member states of the EU are the key to more efficient sanctioning and enforcement through administrative fines.

Keywords: GDPR; European Data Protection Law; sanctions; administrative fines, enforcement; DPAs

Recommended citation: Sebastian J. Golla, Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, 8 (2017) JIPITEC 70 para 1.

A. The Current Lack of Enforcement and Sanctions in Data Protection Law

1 It is common sense that the enforcement of Data Protection Law in Europe needs improvement.[1] A lack of effective sanctions has frequently been cited as one of the main reasons for existing enforcement deficits.[2] In general, effective sanctions are regarded as a prerequisite for achieving compliance with legal rules[3] and in theory, many different types of sanctions can be applied for violations of Data Protection Law, both under the existing national rules and the rules of the GDPR. In practice, however, the application of the sanctions is lagging behind the theoretical possibilities. Accordingly, Data Protection Laws are sometimes referred to as "toothless" or as "paper tigers".[4] From the perspective of legal philosophy, it can even be argued that a law without effective sanctions is not a law at all.

2 This article looks into the possible reasons for the lack of sanctions for violations of data protection rules, and focuses particularly on administrative fines. Specifically, the article examines the new rules of the GDPR concerning administrative fines

1 European Union Agency for Fundamental Rights, *Access to data protection remedies in EU member states* (Publications Office of the European Union, 2013), pp. 11 ff.; Thorben Burghardt and others, 'A Study on the Lack of Enforcement of Data Protection Acts' (Next Generation Society. Technological and Legal Issues - Third International Conference, e-Democracy 2009, Athens, Greece, September 2009); David Wright, 'Enforcing Privacy' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer 2016), pp. 13 ff.

2 Benedikt Buchner, *Informationelle Selbstbestimmung im Privatrecht* (Mohr Siebeck 2006), p. 299; Thomas Hoeren, 'Datenschutz als Wettbewerbsvorteil' in Erich Greipl (ed.), *100 Jahre Wettbewerbszentrale* (Deutscher Fachverlag 2012) p. 135, 136.

3 Thomas Raiser, *Grundlagen der Rechtssoziologie* (6th edn, Mohr Siebeck 2013), p. 253.

4 Jan Philipp Albrecht, 'Regaining Control and Sovereignty in the Digital Age' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer 2016), p. 473, 483; European Union Agency for Fundamental Rights, supra note 1, p. 47.

and attempts to forecast to what extent those rules may be able to compensate for the existing lack of enforcement and sanctions.

I. Administrative Fines and Other Sanctions

3 There are many different legal instruments to sanction violations of Data Protection Law. In a broad sense, a sanction can be defined as "the detriment, loss of reward, or coercive intervention annexed to a violation of a law as a means of enforcing the law".[5] In the context of Data Protection Law, this can include measures from the negative mentioning of a data controller in a supervisory authority's activity report ("naming and shaming") or an order by such an authority, as well as a civil-rights claim for damages by a data subject. Even though immaterial damages such as loss of reputation due to a mention in an activity report or a high-damage claim can be more painful for an enterprise in certain cases, technically administrative fines and criminal penalties are to be regarded as the most severe sanctions for data protection violations.

4 This article focuses on administrative fines for data protection violations. Administrative fines are of a higher practical relevance than criminal penalties.[6] While the Data Protection Directive 95/46/EC (DPD) does not specifically mention or require administrative fines for Data Protection violations,[7] most EU member states have implemented such sanctions in their Data Protection Acts.[8] However, there are big differences in the maximum amounts of administrative fines between the different member states.[9] While Romanian Law (maximum circa 11,000 €)[10] and Slovenian Law (12,510 €)[11] allow for relatively low fines, Spanish (600,000 €)[12] and UK Laws (500,000 £)[13] have much higher thresholds.

II. Deficits in the Application of Administrative Fines

5 In this section, I discuss the possible reasons behind the deficit of sanctions with a particular focus on the application of administrative fines.[14] Hereby I especially look at the role of the data subjects and the sanctioning authorities. For the sake of improved comprehensibility, this article operates under the assumption that DPAs have the competence to impose administrative sanctions for data protection violations, as is the case with most DPAs in Europe.[15]

1. Lack of Interest and Resources

6 If data subjects or authorities gain knowledge of a violation of Data Protection rules, it is their responsibility to initiate a procedure, which can eventually lead to an administrative fine. However, there are several reasons why the involved actors often do not make such an effort.

a.) The Role of Data Subjects

7 First, there are different conceivable reasons for data subjects to avoid initiating proceedings that could lead to administrative sanctions for data controllers. Among the very limited empirical material on the matter, a recent study conducted by the European Union Agency for Fundamental Rights gives some insight into the question.[16] The study looks at the factors that prevent subjects from seeking remedies or initiating procedures after they have experienced data protection violations.[17] Several

5 *Merriam-Webster's Collegiate Dictionary* (11th edn, 2004).

6 European Union Agency for Fundamental Rights, supra note 1, p. 21, Sebastian J. Golla, *Die Straf- und Bußgeldtatbestände der Datenschutzgesetze* (Duncker & Humblot 2015), pp. 199 ff.

7 Art. 24 DPD leaves the regulation of administrative fines at the discretion of the member states; cf. Paul De Hert and Gertjan Boulet, 'The Co-existence of Administrative and Criminal Law Approaches to Data Protection Wrongs' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer 2016), pp. 359 ff.

8 Paul De Hert and Gertjan Boulet, supra note 7, pp. 361 ff. give an overview of criminal penalties and administrative fines.

9 Cf. European Union Agency for Fundamental Rights, supra note 1, p. 21.

10 Maximal fine of 500 million Romanian leu under Art. 33 Law No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data.

11 Article 91 Personal Data Protection Act.

12 Article 45 para. 3 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

13 The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 para. 2.

14 Cf. for a more detailed analysis Sebastian J. Golla, supra note 6, pp. 213 ff.

15 There are, of course, exceptions in certain states such as Kosovo (cf. Njomeza Zejnullahu, 'Imposition of Monetary Sanctions as a Mechanism for Protection of Personal Data: Comparative Analysis of Kosovo and Slovenia' (2016) 2 Eur. Data Prot. L. Rev. 80, 82), Austria (cf. Paul De Hert and Gertjan Boulet, supra note 7, p. 363) or the German State Baden-Württemberg.

16 European Union Agency for Fundamental Rights, supra note 1.

17 European Union Agency for Fundamental Rights, supra note 1, pp. 30 ff.

of these explanations apply to administrative fine proceedings in particular. The study distinguishes between "[I]ssues related directly to the procedure" such as the duration and the costs of the procedure, a "[l]ack of information or knowledge", and "[s]pecific personal and other reasons that made individuals uneasy about initiating the procedures."[18]

8 In a broader sense, the so-called "rational apathy"[19] or "rational disinterest" of data subjects affected by data protection violations can be identified as the main reason for choosing a path on inaction. From the perspective of the data subject, the effort to initiate a procedure can seem disproportionately large compared to the possible outcome. Violations of Data Protection Laws are often not regarded as important enough to take steps against them, especially if they do not affect financial interests and do not involve "sensitive" areas of life such as financial matters or the workplace.[20]

9 While there are several cases where data protection violations can have immediate effects on data subjects,[21] there seem to be even more scenarios where this is not the case and the impact of a data protection violation will only become perceptible a certain time after the initial violation has taken place. This is connected with the typical characteristic of Data Protection Law to protect individual rights in the forefront of further violations. As the German Constitutional Court has stated in its decisions on the basic right to informational self-determination, which is the basis of German Data Protection Law, "such an endangerment situation can already arise in the run-up to concrete threats to specific legal interests, in particular if personal information can be used and linked in a manner which the person concerned can neither detect nor prevent."[22]

10 Furthermore, the fear of potential unsavoury effects can reflect negatively on the individual's interest in filing complaints and initiating procedures. The potential unsavoury effect of an "emotional burden" can be a reason to avoid filing complaints.[23] Second, the fear of negative consequences inflicted by another party can also impede potential complainants.[24] This especially applies in cases where data subjects and violators are in a relationship of dependency.[25] The classic example for this is the situation where the data subject is the violator's employee fearing dismissal if a data protection violation is reported.

11 Individual apathy can especially become a problem in the case of data protection violations with a wide "scatter band", that is, in cases where the violation affects many persons but only has a negligible effect on each single individual.[26] While it may seem rational for each single individual to refrain from filing a complaint, the cumulative effect as such would require a sanction.

b.) The Role of Data Protection Authorities

12 While DPAs can help to compensate for the disinterest on the part of the data subjects, this is only possible to a certain extent. A big share of the work of DPAs is following up on complaints made by citizens. This means that if a data subject does not turn to an authority to initiate a procedure, the chances that a data protection violation is fined significantly decrease. The staffing capacities of authorities often do not allow them to conduct investigations out of their own initiative.

13 Other aspects that can stand in the way of imposing fines follow from the legal mandates of DPAs and their organisation. The main task of DPAs is to operate as a supervisory authority. At the same time, imposing fines for data protection violations is not a classical supervisory task. Supervisory activities are rather based on a cooperative and consulting approach. Those supervisory activities require a certain mutual trust between authorities and data controllers, which can hardly be established if there is a latent threat of imposing administrative fines.[27] Most data protection authorities do not strictly differentiate between their supervisory and sanctioning functions.[28] This leads to a conflict of objectives within the authorities.[29]

14 Several authorities have made it clear that their priority, rather than repressive action, is the

18 European Union Agency for Fundamental Rights, supra note 1, p. 30.

19 Kai von Lewinski 'Zwischen rationaler Apathie und rationaler Hysterie – Die Durchsetzung des Datenschutzes' (2013) 1 Privacy in Germany 12.

20 Cf. European Union Agency for Fundamental Rights, supra note 1, p. 30.

21 Cf. with several examples European Union Agency for Fundamental Rights, supra note 1, p. 28.

22 BVerfGE 120, 274, 312.

23 European Union Agency for Fundamental Rights, supra note 1, p. 30.

24 European Union Agency for Fundamental Rights, supra note 1, p. 32.

25 European Union Agency for Fundamental Rights, supra note 1, p. 30; Thilo Weichert, 'Datenschutzstrafrecht - ein zahnloser Tiger?' (1999) 19 NStZ, 490, 492.

26 Benedikt Buchner, supra note 2, p. 311.

27 Cf. Thilo Weichert, 'Regulierte Selbstregulierung – Plädoyer für eine etwas andere Datenschutzaufsicht' (2005) 21 Recht der Datenverarbeitung 1, 5.

28 One exception is the Bavarian Data Protection Authority which has made this distinction perfectly clear to the public, Bavarian Data Protection Authority, *Activity report 2010/2011*, p. 94.

29 See in more detail Sebastian J. Golla, supra note 6, pp. 216 ff.

prevention of future violations by cooperating with data controllers.[30] Consequently, the discretion of these authorities in imposing sanction is strongly influenced by the cooperative and consulting approach, which leads to a restrained practice.[31] In recent years, however, several authorities have begun to focus more on the enforcement of Data Protection Laws and have stated that they are making more use of their sanctioning competences.[32] This development has been reflected in the recent increase in fines for Data Protection violations in Europe.[33] One example for this changing practice is the UK. The Information Commissioner's Office (ICO) as the country's competent DPA, which has had the power to impose fines since April 2010, had only sparsely imposed administrative fines in the past.[34] However in October 2016, the recently appointed Information Commissioner Elizabeth Denham imposed a record fine of £400,000 against the telecommunications provider TalkTalk.[35] In her first speech as Information Commissioner, Denham said that "[t]he ICO will do its bit by focusing our advisory, education, investigatory and enforcement work on consumer control, transparency and fairness", but also pointed out the possibilities to impose high administrative fines under the GDPR and announced an intent to "use the stick in the cupboard when necessary."[36]

15 In contrast, a European example for a changing approach from strict administrative fines towards less rigid sanctions is the Spanish DPA Agencia Española de Protección de Datos (AEPD). While the AEPD is traditionally among the most active DPAs in Europe in terms of imposing administrative sanctions,[37] the number of cases and the amount of fines has been decreasing over the past years.[38] This is to some extent due to legal reforms,[39] but also because of the AEPD's exercise of discretion. In its latest report for the year 2015, the AEPD announced that it continued its tendency towards a decrease in administrative fines, planning to use other measures to correct data protection violations and to rather implement administrative sanctions as an ultima ratio.[40]

16 To avoid the described conflict of objectives and to enable the authorities to act both in a preventive and repressive manner, a clear separation between those two functions would be necessary. However, this separation proves to be difficult from a practical point of view. Authorities do not have the necessary budget or manpower to keep this tasks seperate and to focus more on imposing administrative fines.[41] Some smaller DPAs have a hard time making use of their very sanctioning competences in the first place.[42]

2. Lack of Information, Lack of Awareness and Legal Uncertainty

17 While a decision in favour of "rational apathy" requires knowledge and awareness that a data protection violation has occurred, in several cases even this requirement is lacking. Lack of information regarding existing rules and a corresponding lack of

30 For instance Hamburg Commissioner for Data Protection and Freedom of Information, *23. Tätigkeitsbericht Datenschutz 2010/2011*, p. 197; North Rhine-Westphalia Commissioner for Data Protection and Freedom of Information, *21. Datenschutz- und Informationsfreiheitsbericht 2011/2012*, p. 19; Independent Centre for Privacy Protection Schleswig-Holstein, *34. Tätigkeitsbericht 2013*, p. 24.

31 Matthias Lindhorst, *Sanktionsdefizite im Datenschutzrecht* (Peter Lang 2010) 42.

32 Alexander Dix, 'The International Working Group on Data Protection in Telecommunications: Contributions to Transnational Privacy Enforcement' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer 2016), p. 183; cf. Berlin Commissioner for Data Protection, *Jahresbericht 2009*, p. 85: "Due to the increasing number of uncovered massive data protection violations, we have given up the rather restrictive application of administrative fines as an ultima ratio in the last years."

33 Paul De Hert and Gertjan Boulet, supra note 7, pp. 364 f.

34 European Union Agency for Fundamental Rights, supra note 1, p. 21; Hazel Grant and Hannah Crowther, 'How Effective Are Fines in Enforcing Privacy?' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer 2016), pp. 287 f.

35 ICO, 'TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack' (*ICO*, 5 October 2016) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/> accessed 29 October 2016.

36 Elizabeth Denham, 'Transparency, trust and progressive data protection' (*ICO*, 29 September 2016) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/09/transparency-trust-and-progressive-data-protection/> accessed 29 October 2016.

37 Artemio Rallo Lombarte, 'The Spanish Experience of Enforcing Privacy Norms: Two Decades of Evolution from Sticks to Carrots' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer 2016), p. 123 ff.; cf. also European Union Agency for Fundamental Rights, supra note 1, p. 21.

38 Agencia Española de Protección de Datos, *Memory 2015*, p. 36.

39 Artemio Rallo Lombarte, supra note 37, p. 123, 137 ff.

40 Agencia Española de Protección de Datos, supra note 38, p. 35 f.

41 Corinna Holländer, 'Datensündern auf der Spur, Bußgeldverfahren ungeliebtes Instrument der Datenschutzaufsichtsbehörden? ' (2009) 25 Recht der Datenverarbeitung 215, 222; Thilo Weichert, supra note 27 1, 6; cf. also European Union Agency for Fundamental Rights, supra note 1, p. 46.

42 For instance, the DPA of the German state Brandenburg only has one part-time employee to prosecute administrative offences; Commissioner of the State of Brandenburg for Data Protection and Access to Information, *16. Tätigkeitsbericht 2010/2011*, p. 158.

awareness in the data subjects are further reasons that can prevent administrative fine proceedings from being initiated. The recent study by the European Union Agency for Fundamental Rights has concluded that "[m]ost people do not know where to find information on the laws governing data protection violations and appropriate remedies, and are not aware of the organisations and institutions offering legal advice and support."[43]

18 Another issue that affects the application of administrative fines and other sanctions is the high degree of legal uncertainty in Data Protection Law. Many regulations operate with terms which leave a lot of room for interpretation. It is often hard to predict whether the processing of personal data is legal. Determining this often requires a balance of the affected interests in a single case.[44] This uncertainty has a negative impact on the possibility of effective compliance. Additionally, it can lead to a restrained use of sanctions. First, the data subjects will have a hard time determining whether a violation has occurred, which can prevent them from filing complaints. Second, working with uncertain rules makes it more difficult for DPAs to justify administrative fines. The concerns of some DPAs regarding the uncertainty of Data Protection Laws might even go so far that the rules of Data Protection Law are not applied due to the assumption that they might violate the constitutional rule of law.

B. Changes under the GDPR

19 The GDPR focuses on effective sanctions for data protection violations. Already in November 2010 the Commission announced in a Communication that it was seeking to "assess the need for strengthening the existing provisions on sanctions, for example by explicitly including criminal sanctions in case of serious data protection violations, in order to make them more effective."[45] Recitals 11 and 13 of the GDPR state that equivalent sanctions for data protection infringements are one essential requirement to ensure the "[e]ffective protection of personal data throughout the Union" and "a consistent level of protection for natural persons throughout the Union."

20 In this section, I briefly discuss the administrative fines newly introduced by the GDPR. Then I discuss to what extent the new rules of the GDPR may be able to address the current challenges.

I. The New Administrative Fines

21 The administrative fines under Article 83 GDPR are the strongest sanctioning instrument directly provided by the regulation. The fines that go up to 20,000,000 €, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, have received a lot of public attention. They have been interpreted as a legislative signal to US-American internet enterprises such as Alphabet or Facebook.[46] The fines in Article 83 GDPR are exceeding the fines in national laws both in the maximum amounts and in scope for offences entailing either negligent or intentional conduct. Even if this is not explicitly stated in Article 83 GDPR, it follows from the principle of culpability enshrined in Article 48 paragraph 1, Article 49 paragraph 3 Charter of Fundamental Rights of the European Union.

1. The Offences

22 Article 83 paragraphs 4 – 6 GDPR mainly cover data protection violations by controllers (Article 4 (7) GDPR) and processors (Article 4 (8) GDPR). The administrative offences refer to approximately 50 provisions of the GDPR.

23 Offences under Article 83 paragraph 4 GDPR are subject to administrative fines of up to 10,000,000 €, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year. Paragraph 4 (a) refers to the obligations of controllers and processors in Chapter 4 GDPR. Among many other provisions, the rule refers to Article 25 GDPR, which sets requirements for data protection by design and by default. Other offences, which could potentially become important in practice, include violations of the obligations to cooperate with supervisory authorities (Article 31 GDPR) and to appoint a data protection officer (Article 37 GDPR). Para 4 (b) and (c) include certification bodies (Article 43 GDPR) and monitoring bodies (Article 41 paragraph 1 GDPR) as special addressees for administrative fines.

24 Offences under Article 83 paragraph 5 and 6 GDPR are subject to administrative fines of up to 20,000,000 €, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year. Here, especially paragraph 5 (a) has a broad scope and high relevance. Under paragraph

43 European Union Agency for Fundamental Rights, supra note 1, p. 35.

44 Especially under Article 7 (f) DPD, cf. Sebastian J. Golla, supra note 6, pp. 163 ff.

45 Commission, 'A comprehensive approach on personal data protection in the European Union' COM(*2010*) *609 final*, p. 10.

46 Hazel Grant and Hannah Crowther, supra 34, p. 287, 291.

5 (a) infringements of the basic principles for processing personal data constitute administrative offences. This includes any unlawful processing against Article 6 GDPR. Under paragraph 5 (b) a violation of the rights of the data subject constitutes an administrative offence, paragraph 5 (c) refers to the rules on the transfers of personal data to third countries or international organisations in Chapter V GDPR. Under paragraph 5 (c), violations of member states' provisions, which have been adopted under the opening clauses in Chapter IX GDPR are subject to sanctions. Those provisions potentially include data processing for journalistic purposes and the purposes of academic, artistic or literary expression (Article 85 GDPR) or processing in the context of employment (Article 88 GDPR). Under paragraph 5 lit. (e) the non-compliance with orders of supervisory authorities and the failure to provide access to information are subject to fines. Next to this, the additional offence for the non-compliance with orders by the supervisory authority in paragraph 6 seems redundant.

2. General Conditions for Imposing Administrative Fines and Rules for Discretion

25 In case of a violation, the GDPR considers the imposition of an administrative fine as a rule according to Recital 148 sentence 1. That a fine is not necessary in each case follows from Recital 148 sentence 2, which states that only "[i]n a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine." This novelty in the GDPR is important for the fining practice since it restrains the discretion that authorities might have for imposing sanctions under national laws.[47]

26 According to Article 83 paragraph 1 GDPR, fines "shall in each individual case be effective, proportionate and dissuasive". Those criteria are based on the European Court of Justice's jurisdiction regarding the regulation and imposition of sanctions by member states in the event of violations of Laws of the European Union.[48] To be effective and dissuasive, fines must have a certain preventive effect. However, those criteria leave a lot to the discretion of the competent authorities. The criterion of proportionality requires considering the circumstances of each individual case when imposing a fine.[49] The requirement of proportionality can also be applied in favour of data controllers, protecting them from inadequate fines. For instance, it has to be taken into account which fines have been imposed against competitors in the event of similar infringements.[50] This can be regarded as a specific regulation of the proportionality principle enshrined in Article 49 paragraph 3 Charter of Fundamental Rights of the European Union, which applies to penalties as well as to administrative fines.[51]

27 The requirement of proportionality is also reflected in the criteria in Article 83 paragraph 2 GDPR. The criteria of discretion regulated here concern both the question when an administrative procedure is to be initiated and the admeasurement of the administrative fine at the end of the procedure. The depth of detail with which the criteria of discretion have been regulated is unprecedented for a EU regulation. The criteria are inspired by the Commission's practice of administrative fines in Competition Law under Article 23 paragraph 2 lit. a) Council Regulation (EC) No 1/2003,[52] which is documented in guidelines.[53] According to Article 70 paragraph 1 (k) GDPR, the European Data Protection Board shall also draw up guidelines for supervisory authorities concerning the setting of administrative fines pursuant to Article 83 GDPR.

28 The criteria in paragraph 2 refer to the violation itself ((a), (b) and (g)), the precedent ((d), (e), (i) and (j)) and the subsequent behavior of the violator ((c), (f) and (h)). Beyond that, the general clause in paragraph 2 makes it possible to give regard to any other aggravating or mitigating factor applicable to the circumstances of the case. The principle of proportionality under paragraph 1 as well as the principle of certainty enshrined in Article 49 paragraph 1 Charter of Fundamental Rights of the European Union require a coherent and predictable imposition of administrative fines. In practice, this will require a union-wide cooperation of the competent authorities. According to Recital 150 sentence 5, the consistency mechanism (Article 63 ff. GDPR) may be used to promote a consistent application of administrative fines.

47 For instance, in German Law Section 47 para. 1 Act on Regulatory Offences gives a wider discretion to German authorities to prosecute administrative offences.

48 Case 68/88 *Greek Maize* [1989] ECR I-2965; Case 326/88 *Hansen* [1990] ECR I-2911.

49 Cf. Helmut Satzger, *Die Europäisierung des Strafrechts* (Carl Heymanns 2001) p. 372.

50 Gregor Thüsing and Johannes Traut, 'The Reform of European Data Protection Law: Harmonisation at Last?' (2013) 48 Intereconomics 271, 275.

51 Hans Jarass, *Charta der Grundrechte der Europäischen Union* (3rd edn, 2016), Article 49 para. 7.

52 Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty.

53 Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No 1/2003, paras. 27 ff.

3. Amount of Fines

29 The maximal amount of fines under Article 83 paragraph 4 to 6 has been a controversial subject in the legislative procedure. While Article 79 paragraph 2a (c) GDPR in the Parliament's version contained fines with a maximum amount of 100,000,000 € or of up to 5% of the total worldwide annual turnover of an undertaking, Article 79a GDPR in the Council's version only proposed a maximum of 250,000 € or up to 0.5% of the total worldwide annual turnover for certain violations.

30 Additionally, the calculation of the maximum amount poses some difficulties if it is based on the annual turnover. The practically relevant question is how the term "undertaking" in Article 83 is to be interpreted and if it covers corporate groups (like, for instance, Alphabet Inc.) or only single (subsidiary) companies.[54] The high economical relevance of this question becomes clear when looking at the large differences between turnovers of corporate groups and single companies.

31 According to Recital 150 sentence 3, "where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes." The term "undertaking" in Articles 101 and 102 TFEU is interpreted in a broad sense by the European Commission and the European Court of Justice. In the context of Competition Law the economic activity is decisive for the understanding of the term "undertaking".[55] In the words of the European Court of Justice, "the concept of an undertaking encompasses every entity engaged in an economic activity, regardless of the legal status of the entity and the way in which it is financed".[56] Therefore, "undertakings" in European Competition Law have been defined as "economic units which consist of a unitary organization of personal, tangible and intangible elements which pursues a specific economic aim on a long-term basis".[57] This can include entities consisting of multiple natural or legal persons.[58] In particular, a parent company and a subsidiary are to be considered an economic unit if the "subsidiary does not decide independently upon its own conduct on the market, but carries out, in all material respects, the instructions given to it by the parent company".[59]

32 However, one can also interpret the term "undertaking" similar to the term "enterprise" in Article 4 (18) GDPR. This would mean that only one natural or legal person could be regarded as an "undertaking", but not a group of companies. This interpretation is supported by the fact that several language versions of the GDPR use an identical term for what is described as an "undertaking" in Article 83 GDPR and as an "enterprise" Article 4 (18) GDPR (English version).[60]

33 Nonetheless, the interpretation following Recital 150 sentence 3 clearly corresponds with the legislator's will. The use of identical terms in Article 4 (18) GDPR and Article 83 GDPR in several language versions seems technically flawed and unfortunate. Recitals may specify the operative part of a regulation but may not establish incoherencies.[61] Here, the interpretation of Article 83 GDPR according to Recital 150 sentence 3 does not seem incoherent with Article 4 (18) GDPR. The rules of the GDPR are to "be interpreted and applied in the light of the versions existing in the other official languages"[62] to achieve a uniform interpretation. The different language versions show that the terms in Article 4 (18) GDPR and Article 83 GDPR are not necessarily identical, since several language versions use different terms in both provisions.[63]

34 As a result, "undertakings" under Article 83 GDPR can consist of several legal persons. Therefore, the total turnover of a corporate group will be decisive for the calculation of an administrative fine.[64]

54 Cf. Kai Cornelius, 'Die datenschutzrechtliche Einheit als Grundlage des bußgeldrechtlichen Unternehmensbegriff nach der EU-DSGVO' (2016) 5 Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht 421 ff.; Sebastian Faust, Jan Spittka and Tim Wybitul, 'Milliardenbußgelder nach der DS-GVO? Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz' (2016) 6 Zeitschrift für Datenschutz 120; Gerald Spindler, 'Die neue EU-Datenschutz-Grundverordnung' (2016) 69 Der Betrieb 937, 946 f.

55 Wolfgang Weiß, Art. 101 AEUV in Christian Calliess and Matthias Ruffert (eds), *EUV/AEUV* (C.H. Beck 2016), para. 25.

56 Case C-41/90 *Höfner and Elsner* [1991] ECR I-1979; cf. also Case C-205/03 P *FENIN* [2006] ECR I-6295.

57 Case T-11/89 *Shell* [1992] ECR II-757; cf. Wolfgang Weiß, supra note 55, para. 25.

58 Cf. Case 48/69 *Imperial Chemical Industries* [1972] ECR 619.

59 Case C-97/08 P *Akzo Nobel* [2009] ECR I-8237.

60 The German version for instance uses the term "Unternehmen" in both provisions. The French, Spanish and Italian version also use identical terms.

61 Case C-344/04 *International Air Transport Association* [2006] ECR I-403.

62 Case C-484/14 *McFadden* [2016].

63 Besides the English version, for instance the Bulgarian version uses different terms in Art. 83 ("предприятие") and Art. 4 (18) ("дружество") GDPR.

64 This opinion is shared by the Bavarian Data Protection Authority, 'Sanktionen nach der DS-GVO' (*BayLDA* 1 September 2016) <www.lda.bayern.de/media/baylda_ds-gvo_7_sanctions.pdf> accessed 29 November 2016.

II. Chances to Compensate Existing Deficits

35 The new rules of the GDPR and the ones on administrative fines in particular, have brought a lot of promises. For instance, Jan Philipp Albrecht, a Green Party MEP who was leading the negotiations between the Parliament and the Council on the adoption of the GDPR, has recently declared that with the application of the GDPR from 24 May 2018, "the lack of enforcement in the field of data protection provisions will end."[65] This section analyses to what extent the new legal rules have the potential to compensate the deficits described above.

1. Lack of Interest and Resources

36 The regulation of administrative fines in the GDPR does little to compensate for the lack of interest and resources of data subjects and DPAs in initiating procedures to fine data protection violations. Naturally, the potential of legal rules is limited in this regard. Looking at individual data subjects as potential complainants, it is difficult to create an environment that would encourage data subjects to initiate administrative fining procedures by legal rules since complainants do not economically profit from a successful procedure. However, complaints may slightly increase due to the more detailed rules on the DPA's discretion to impose fines in Article 83 paragraph 2 GDPR. A clearer and more predictable procedure might have positive effects on an individual's motivation to file complaints and to initiate procedures.

37 On the side of the DPAs, there are several issues which cannot be solved by the European regulation itself. In particular, the personal and financial resources of DPAs remain a problematic issue. One aspect that is tackled by the GDPR however is the conflict of objectives between the supervisory and fining functions of authorities described above. Again, the new rules about the discretion to impose sanctions in Article 83 paragraph 2 GDPR are a positive development to compensate for existing deficits. They are a first step towards a more effective union-wide cooperation between DPAs. They also might improve the sanctioning practices and mitigate the existing conflict of objectives. The fact that national data protection laws mostly do not offer specific guidance regarding administrative sanctions practices[66] entices DPAs to apply the standards of supervisory work to sanctioning work, which has led to a restrained practice so far.

38 Nonetheless, the GDPR does not distinguish clearly enough between the sanctioning and supervisory functions of the authorities. Article 58 paragraph 2 (i) and 83 paragraph 1 GDPR regard the imposition of administrative fines as one of several corrective powers of the DPAs as supervisory authorities. A stronger and clearer legal distinction between the functions as supervisory and sanctioning authorities would have been helpful to make this difference clearer.

2. Lack of Information, Lack of Awareness, and Legal Uncertainty

39 Regarding the issues of information, awareness, and legal certainty, the GDPR only partially helps to compensate for the deficits described above. Certainly, the GDPR and its legislative procedure have already raised the awareness for Data Protection Law and the potentially high fines. For instance, in a global survey report by the analyst firm Ovum in 2015, 52% of 366 IT decision makers said that they were expecting fines for their company under the GDPR.[67]

40 However, in terms of legal certainty, the GDPR is helpful only to a certain extent. On the one hand, the legal certainty will increase for enterprises that operate globally or in several European states since the substantial rules of Data Protection Law and the enforcement practices undergo a harmonisation. On the other hand, for smaller players, some DPAs, and also from the citizens' perspective, the new rules for administrative fines may become even harder to predict compared to the existing national laws. The reason for this is that the administrative offences under Article 83 paragraph 4 and 5 GDPR are extremely vague and unclear. Many of the almost 50 rules of the GDPR to which the offences refer do not draw a sufficiently clear line between legal and illegal behaviour.

41 For instance, Article 83 paragraph 4 a) in conjunction with Article 25 GDPR, which provides fines for infringements on the requirements for privacy by design and by default, does not seem compatible with the principle of certainty. From the criteria formulated in Article 25 paragraph 1 and 2 GDPR, the addressee of the rule will not be able to foresee if the measures they take fulfill the requirements of these rules.[68] The regulation does not provide a clear

65 Jan Philipp Albrecht, 'How the GDPR Will Change the World' (2016) 2 Eur. Data Prot. L. Rev. 287.

66 Paul De Hert and Gertjan Boulet, supra note 7, p. 364.

67 Ovum, *Data Privacy Laws: Cutting the Red Tape* (Report, 2015).

68 Malaika Nolde, 'Sanktionen nach der EU-Datenschutzgrundverordnung' in Jürgen Taeger (ed.), *Smart World – Smart Law?* (OIWIR 2016) 757, 768.

standard and does not answer the question regarding which technical and organisational measures are to be considered appropriate in an individual case to implement data-protection principles of the GDPR. In a similar manner, Article 83 paragraph 5 a) in conjunction with Article 6 paragraph 1 (f) GDPR fails to provide the addressee of the rules with sufficiently clear information on which conduct can be subject to a fine. According to Article 6 paragraph 1 (f) GDPR, the legality of processing personal data will depend on the result of a balance of interests in the individual case. Without further legal guidance, the outcome of this balance of interests will hardly be predictable in the majority of cases.

C. Conclusion: A Potential Game Changer but No Instant Cure

42 To conclude, the GDPR and its rules on administrative fines in Article 83 GDPR contain some positive steps to attenuate the existing lack of enforcement and sanctions in Data Protection Law. The GDPR's stronger focus on sanctions compared to the DPD, and especially the new fines, have gained some public attention. Both DPAs and companies in the IT-sector seem to be preparing for a stricter practice of fining. The existing conflict of goals in the DPAs is likely to be attenuated by the more specific rules for the discretion in imposing administrative sanctions. However, the GDPR still does not clearly distinguish between sanctioning and supervisory functions of DPAs. Regrettably, the GDPR also fails to compensate for some other legal problems which stand in the way of the effective sanctioning of Data Protection violations. In particular, the issue of legal uncertainty will cause headaches under the GDPR. Some central provisions to which Article 83 GDPR refers, such as Article 6 paragraph 1 (f) and Article 25 GDPR, do not live up to the principle of certainty and are not suitable for effective practical application.

43 The GDPR has the potential to become a game changer when it comes to sanctions and administrative fines in particular. However, the lack of enforcement will not immediately end with the application of the GDPR, as Jan Philipp Albrecht was quick to announce.[69] Certainly, the GDPR will lead to more frequent and higher fines for Data Protection violations in member states which have been operating on a low level so far.[70] But still, the question whether higher fines will be imposed on a regular basis in all member states remains open. It seems unlikely that eight-figure administrative fines will be imposed on a regular basis. The existence of a higher upper threshold does not necessarily mean that this threshold will ever be reached. In European Competition Law for example, the Commission has not yet exhausted the threshold for administrative fines, which are also calculated on the basis of the annual turnover.[71] All in all, it will require hard work and coordination of the European DPAs to significantly improve the overall situation of enforcement and sanctioning. Growing teeth can be a slow and painful process.

---

* This article is based on findings from the author's PhD thesis *Die Straf- und Bußgeldtatbestände der Datenschutzgesetze* [Criminal and Administrative Offences under Data Protection Acts] (Duncker & Humblot 2015). Since the thesis was submitted before the GDPR was passed and entered into force, the article especially focuses on the differences in the situation before and after the GDPR.

69 Jan Philipp Albrecht, supra 66. It is another question if an absolutely strict enforcement of data protection rules from one moment to another would even be desirable considering potential effects for the economy and freedoms of communication.

70 Hazel Grant and Hannah Crowther, supra 34, p. 287, 302.

71 Gregor Thüsing and Johannes Traut, supra note 50, 271, 276.

Novel EU Legal Requirements in Big Data Security

Big Data – Big Security Headaches?

by **Jasmien César and Julien Debussche**, the authors are associates at the law firm Bird & Bird LLP, Brussels, toreador@twobirds.com

Abstract: This paper aims to provide an overview of the new legal requirements related to security and breach notification imposed on businesses in the European Union and to demonstrate their pertinence for big data service providers. In addition, it lays down practical recommendations for the implementation of those requirements into the internal security strategies of big data service providers.

Keywords: Big data; security; breach notification; legal obligations

Recommended citation: Jasmien César and Julien Debussche, Novel EU Legal Requirements in Big Data Security: Big Data – Big Security Headaches?, 8 (2017) JIPITEC 79 para 1.

A. Security

1 As highlighted by the European Commission in its Communication "Towards a thriving data-driven economy", we currently observe a new industrial revolution driven by digital data, computation and automation.[1] Human activities, industrial processes, and research all engender the collection and processing of data in unprecedented proportions, triggering new products and services as well as new business processes and scientific methodologies.[2]

2 The resulting datasets, or "big data", are prone to security risks and incidents. In recent times, instruments have emerged to prevent or adequately respond to such risks, thereby imposing obligations on different actors in the data value cycle.

3 Such obligations not only derive from the General Data Protection Regulation (the GDPR), but also from other legislative instruments at both the European Union (EU) and national level. The advent of the (minimal harmonisation) Network Information Security Directive (the NIS Directive, also known as the Cyber-security Directive) has multiplied the requirements relating to security and cyber-security.

I. Requirements under the General Data Protection Regulation

4 For most big data analytics, it cannot be excluded that a processing of personal data will take place. In such case, the requirements relating to security under the GDPR will apply.

5 The obligations under the GDPR in relation to security are closely linked to those under the NIS Directive examined below, and are in line with best practices applicable to information society systems that require adequate protection of assets.

1 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a thriving data-driven economy", 2 July 2014, COM(2014) 442 final.

2 Ibid.

1. Data Governance Obligations

6 Under the GDPR, any organisation must implement a wide range of measures to reduce the risk of non-compliance with the GDPR and to prove that it takes data governance seriously. Such measures create significant operational obligations and costs.

7 A general obligation is imposed upon data controllers* to adopt technical and organisational measures to meet the requirements set in the GDPR and to be able to demonstrate that they have done so (Article 24 of the GDPR). Operating a regular audit programme, implementing privacy-by-design measures, running a Privacy Impact Assessment, appointing a Data Protection Officer, etc. are all measures considered to be in line with the data governance obligations, including the security-related requirements. Such measures must be reviewed and updated on a regular basis, taking into account the changing circumstances (Article 24(1) of the GDPR).

8 Furthermore, it shall be considered that the GDPR imposes a high duty of care upon data controllers in selecting their personal data processing service providers, which will require procurement processes and request for tender documents to be regularly assessed, in particular on the security aspects (Article 28 of the GDPR).

9 Adherence by the data controller or processor to an approved code of conduct or certification mechanism may feature as an element to demonstrate compliance with such data governance obligations (Articles 24(3) and 28(5) of the GDPR).

2. Security of Data Processing

10 The GDPR requires data controllers and processors to implement "technical and organisational measures to ensure a level of security appropriate to the risk" (Article 32 of the GDPR).

11 Such measures shall take into account the following elements:

- the state of the art;
- the costs of implementation;
- the nature, scope, context, and purposes of the processing; and
- the risk of varying likelihood and severity for the rights and freedoms of natural persons.

12 In assessing the appropriate level of security, account shall be taken in particular of the risks presented by the processing, notably from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed (Article 32(2) of the GDPR).

13 In this respect, the GDPR provides the following specific suggestions for what types of security measures may be considered "appropriate to the risk" (Article 32(1) of the GDPR):

- the pseudonymisation and encryption of personal data;
- the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

14 The GDPR indicates that adherence to an approved code of conduct or certification mechanism may be used as an element to demonstrate compliance with the security requirements (Article 32(3) of the GDPR). Currently, such codes of conduct or certification mechanisms are not yet on the market. In the absence of such instruments, companies shall rely on best practices and guidance provided by the authorities and take into account the elements mentioned above.

II. Requirements under the Network Information Security Directive

1. Context

15 The NIS Directive was adopted on 6 July 2016 and entered into force in August 2016. From then on, EU Member States have 21 months to transpose the Directive into their national laws and 6 additional months to identify the providers of essential services subject to the Directive's requirements (Article 25 of the NIS Directive).

2. Scope of Application

16 The Directive imposes (online) security obligations on providers of two different types of services discussed below: essential and digital services.

a.) Essential Service

17 Article 5 of the NIS Directive defines an essential service as "a service essential for the maintenance of critical societal and/or economic activities depending on network & information systems, an incident to which would have significant disruptive effects on the service provision."

18 EU Member States have to identify the operators of essential services established on their territory within 27 months after entry into force of the Directive. Operators active in the following sectors may be included: energy, transport, banking, stock exchange, healthcare, utilities, and digital infrastructure (Annex II to the NIS Directive).

19 When determining the significance of a disruptive effect in order to identify operators of essential services, the EU Member States must consider the following factors (Article 6 of the NIS Directive):

- the number of users relying on the service concerned;
- the dependency of (one of) the sectors mentioned above regarding the service concerned;
- the impact incidents could have on economic and societal activities or public safety;
- the market share of the entity concerned;
- the geographic spread of the area that could be affected by an incident;
- the importance of the entity to maintain a sufficient level of the service, taking into account the availability of alternative means for the provision of that service;
- and any other appropriate sector-specific factor.

b.) Digital Service

20 A digital service is described as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" (Article 4(5) of the NIS Directive).

21 The NIS Directive covers three different types of digital services, which are defined as follows (Article 4 of the NIS Directive):

- Online marketplace: "a digital service that allows consumers and/or traders to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online market place".
- Online search engine: "a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found".
- Cloud computing service: "a digital service that enables access to a scalable and elastic pool of shareable computing resources" (See Fig. 1 below – Recital 17 of the NIS Directive).

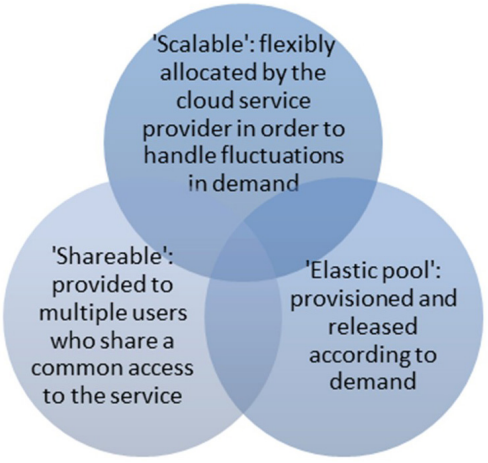

Figure 1: Definition of cloud computing service

22 In contrast to the operators of essential services, which are identified by each EU Member State, online businesses must self-assess whether they are targeted by the rules of the NIS Directive.

23 Considering the above, big data service providers may fall within the scope of the NIS Directive depending on the type of services they provide and the type of sector they are active in. It shall also be noted that, even though the NIS Directive only explicitly targets essential and digital service providers, suppliers to such providers may also be impacted by the obligations under the Directive due to flow down obligations.

3. Overview of New Rules

24 Given its nature as a Directive, the NIS Directive will need to be transposed into national law by the EU Member States. In the context of big data analytics, the essential and digital service providers and – where applicable – their suppliers will therefore need to comply with the transposing national law

in the EU Member State where they are established.

25 A digital service provider that is not established in the EU but providing services within the EU must appoint a representative. This representative will need to be established in one of the EU Member States where the digital services concerned are offered. In that case, the digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established (Article 18(2) of the NIS Directive).

26 Under the new rules intended to improve online security, the essential and digital service providers will notably have to (i) interact with new key actors; (ii) implement security measures; and (iii) notify security incidents.

a.) Interaction with New Key Actors

27 The NIS Directive requires EU Member States to designate several new actors with the aim of attaining a high common level of security of network and information systems within the EU (Article 1(1) of the NIS Directive).

28 Thus, each EU Member State has to designate one or more national competent authorities (NCAs) on the security of network and information systems, who shall monitor the application of the NIS Directive at the national level (Article 8(1) of the NIS Directive). Other key players coming onto the scene are the Computer Security Incident Response Teams (CSIRTs) (Article 9 of the NIS Directive). Interactions with such entities notably include the requirement to notify security incidents either to the NCAs or to the CSIRTs. The NCAs will have the necessary powers to urge essential and digital service providers to comply with their obligations under the NIS Directive (Articles 15 and 17 of the NIS Directive).

29 Furthermore, each EU Member State must select a national single point of contact, in order to facilitate the cross-border cooperation between the NCAs, the CSIRTs, and other relevant national authorities. If an EU Member State decides to designate only one NCA, that NCA will also perform the function of single point of contact (Article 8(3) of the NIS Directive).

b.) Implementation of Security Measures

30 The NIS Directive further requires operators of essential services and digital service providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the networks and information systems that they use for the provision of their services, and to prevent and minimise the impact of incidents affecting the security of such network and information systems (Articles 14 and 16 of the NIS Directive).

31 The security measures shall take into account the state of the art, to ensure a level of security of network and information systems that are adequate to the risk. Digital service providers must also consider the following specific elements when determining the appropriate security measures (Article 16(1) of the NIS Directive):

- the security of systems and facilities;
- incident handling;
- business continuity management;
- monitoring, auditing and testing;
- and compliance with international standards.

c.) Notification of Security Incidents

32 Under the NIS Directive, operators of essential services and digital service providers must notify the NCA or the CSIRT of incidents that have a significant impact on the continuity or provision of the services without undue delay (see Section A.II below for more details).

III. Security Standards

33 In addition to legal requirements on security, security standards indisputably have an important role to play in big data analytics. Moreover, relying on standards and certification schemes facilitates demonstrating compliance with legal requirements, including security requirements.

34 By relying on existing schemes, such as for instance the ISO/IEC 27000 series issued by the International Standards Organisation (the ISO) and the International Electrotechnical Commission (the IEC), big data service providers can demonstrate to the regulator and to their customers that their systems are adequate in terms of security.

35 Furthermore, several standards development organisations have created and are currently developing big data-specific standards. It is essential for any big data service provider to follow the evolutions in this respect closely.

IV. Security throughout the Data Value Cycle

36 The implementation of the abovementioned security measures can only make sense if they are implemented holistically, at all different stages of the data value cycle, to guarantee the continuity of services.[3] Fig. 2 aims to depict the data value cycle.[4]

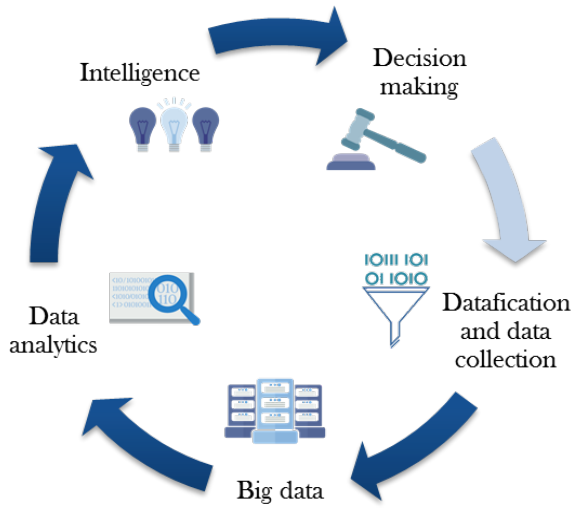

Figure 2: Data value cycle

37 Concretely, such a holistic approach entails that the following specific security issues and their possible mitigation measures ought to be considered throughout the different stages depicted above:[5]

Security issues	Mitigation measures
Integrity of the devices collecting data	Security testing procedures and audits, compliance with standards and certification mechanisms, access control and authentication.
Source validation	Encryption, security testing procedures and audits, risk assessment, source filtering, access control and authentication, monitoring and logging.
Infrastructure security	Security testing procedures and audits, compliance with standards and certification mechanisms, source filtering, access control and authentication, monitoring and logging.
Data security & secure data management	Encryption, security testing procedures and audits, access control and authentication, monitoring and logging.
Platform (e.g., cloud) security	Encryption, security testing procedures and audits, compliance with standards and certification mechanisms, risk assessment, access control and authentication, monitoring and logging.
Supply chain security	Security testing procedures and audits, compliance with standards and certification mechanisms, risk assessment.
Application software security	Security testing procedures and audits, compliance with standards and certification mechanisms, access control and authentication.
Interoperability of applications	Security testing procedures and audits, compliance with standards and certification mechanisms, access control and authentication.
Distributed denial-of-service attacks	Security testing procedures and audits, source filtering, monitoring and logging.
Unauthorised access	Encryption, security testing procedures and audits, compliance with standards and certification mechanisms, access control and authentication, monitoring and logging.

Table 1: Security issues and mitigation measures

38 In addition to applying mitigation measures internally, any company should ensure that safeguards are included in its contracts with, and can be enforced against, possible business partners.[6] Any such agreement should therefore contain specific information security obligations as well as the warranties, indemnity provisions, and limitations of liability related thereto. In order to ensure the enforceability of such clauses, the contract should also provide for audit rights.[7]

39 Furthermore, and inevitably, any agreement concluded for information security purposes should incorporate a comprehensive confidentiality clause.[8]

40 Better still, before entering into any business relations, an exhaustive due diligence of the envisaged business partner should be carried out, with a particular focus on information security.[9]

3 R Naydenov, D. Liveri, L. Dupre, E. Chalvatzi and C. Skouloudi, "Big data security - good practices and recommendations on the security of big data systems", (ENISA 2015).

4 OECD, "Data-driven innovation: big data for growth and well-being", (OECD Publishing 2015), <http://dx.doi.org/10.1787/9789264229358-en>.

5 R Naydenov, D. Liveri, L. Dupre, E. Chalvatzi and C. Skouloudi, "Big data security - good practices and recommendations on the security of big data systems", (ENISA 2015).

6 MR Overly, "Information security in vendor and business partner relationships" in JR Kalyvas and MR Overly (eds.), *Big Data: A Business and Legal Guide* (Auerbach Publications 2015).

7 Ibid.

8 Ibid.

9 Ibid.

V. Conclusion

41 Big data service providers must thoroughly and recurrently assess whether they are subject to security obligations under the GDPR and/or the NIS Directive.

42 In the affirmative, they shall integrate measures, at all different stages of the data value cycle:

- to ensure a level of security appropriate to the risks posed;
- enabling the on-going confidentiality, integrity, availability and resilience of systems and services (including those processing personal data);
- enabling the ability to restore the availability and access to data in a timely manner in the event of incidents;
- and to regularly test, assess and evaluate the effectiveness of security measures.

B. Breach-related Obligations

43 As an emerging technology, big data tends to rely on highly novel and high tech IT systems, which have had no or little time to fully mature into relatively secure techniques.[10] This not only renders big data systems vulnerable against external attacks, but also exposes it to potential unintentional data leaks.

44 The present Section focuses on the legal obligations that apply when data is thus compromised.

I. Preliminary Remark

45 Firstly, it should be noted that the legal concept of "data breach" does not coincide with the technical definition of "data breach".

46 As elaborated by E. Damiani in a big data context, there exist two sub-categories of threats on a technical level; i.e. (big) data breach and (big) data leak.[11] In this context, data breach refers to the theft of a data asset by intruding into the IT infrastructure, whereas data leak covers the disclosure of a data asset at a certain stage of its lifecycle.[12]

47 The legal notion of data breach however, encompasses both technical definitions of data breach and data leak. Indeed, data breach in a legal context does not necessarily entail the malicious behaviour of a third party, but is also established in case (personal) data is disclosed without interference of a threat actor – e.g., losing an unencrypted device.

48 Throughout this paper, we shall use the term "data breach" to refer to its legal interpretation.

II. Notification Obligation under the GDPR

1. Scope of the Obligation

49 The GDPR requires the notification of "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (Articles 4(12) and 33 of the GDPR).

50 The table below provides an overview of the obligations imposed on the different actors involved.

Duty	Timing	Exemption
Data processor to notify data controller	Without undue delay after becoming aware of the data breach.	No exemptions mentioned in the GDPR, but the European Data Protection Board is tasked to issue guidelines on the particular circumstances in which a breach shall be notified.
Data controller to notify supervisory authority	Without undue delay and, where feasible, nolater than 72 hours after having become aware of the data breach.	Notification is not required if the breach is unlikely to result in a risk to the rights and freedoms of individuals.
Data controller to notify affected individuals (in close cooperation with the supervisory authority)	Without undue delay.	Notification is not required if: 1. The breach is unlikely to result in a high risk to the rights and freedoms of individuals; or 2. Appropriate technical and

10 E Damiani, C. A. Ardagna, F. Zavatarelli, E. Rekleitis (ed.) and L. Marinos, "Big data threat landscape and good practice guide", (ENISA 2016).

11 E Damiani, "Toward big data risk analysis", IEEE International Conference on Big Data (IEEE 2015), Santa Clara, CA, pp. 1905-1909.

12 E Damiani, C. A. Ardagna, F. Zavatarelli, E. Rekleitis (ed.) and L. Marinos, "Big data threat landscape and good practice guide", (ENISA 2016).

		organisational protection measures were in place at the time of the incident (e.g. data encryption); or 3. Measures have been taken subsequent to the incident, ensuring that the risk to the right and freedoms of individuals is unlikely to materialise; or 4. It would trigger disproportionate efforts. However, in this case, a public communication or similar measure to inform the public is required.

Table 2: Breach notification requirements under the GDPR

2. Notifications in Practice

51 The breach notification obligation under the GDPR evidently only applies in case of a breach of personal data. Therefore in the event of an incident, it is essential to carefully assess the nature of the data exposed. If such an assessment shows that no personal data has been affected, in principle no data breach notification is required under the GDPR. In this respect, it could reasonably be advocated that a breach of anonymised data or encrypted data – the key for which cannot be retrieved by a third party – does not need to be notified under the GDPR.

52 Therefore, appropriate technical and organisational measures should be implemented to be able to detect promptly whether a personal data breach has taken place and to immediately inform the supervisory authority and the individual if needed (Recital 87 of the GDPR). Such measures include the keeping of good logs, which facilitates a swift and efficient forensic investigation in case of an incident.

53 The personal data breach notification by the data controller to the supervisory authority must at least mention the following information (Article 33(3) of the GDPR):

i. The nature of the breach, including the categories and approximate number of individuals as well as personal data records affected;

ii. The name and contact details of the data protection officer or any other contact point that could provide more information;

iii. The likely consequences of the breach;

iv. The measures (proposed to be) taken by the data controller to address the breach, including any measures to mitigate its negative effects.

54 The communication to the affected individuals must detail in clear and plain language the nature of the personal data breach, recommendations to mitigate possible adverse effects, as well as the information listed under (ii), (iii) and (iv) above (Article 34(2) and Recital 86 of the GDPR).

55 In case it proves impossible to provide such information simultaneously within 72 hours, the GDPR allows providing such information in phases (Article 33(4) of the GDPR). However, the notification should indicate the reasons for the deferment, and the missing information should be provided without further undue delay (Recital 85 of the GDPR).

56 In line with the principle of accountability, the data controller must document any personal data breach as well as the corrective measures taken in order to allow the supervisory authority to assess compliance with the data breach notification obligations (Article 33(5) of the GDPR).

3. Sanctions

57 Under the GDPR, a company that does not comply with the data breach notification obligations may be liable to an administrative fine of up to 10,000,000 Euros or 2 per cent of its total worldwide annual turnover (Article 83(4) of the GDPR). Such a fine is entirely distinct from the affected individual's right to claim compensation for any material or non-material damage suffered as a result of an infringement of the data breach notification obligation (Article 82 of the GDPR).

III. Notification Obligation under the NIS Directive

1. Scope of the Obligation

58 Under the NIS Directive, operators of essential services and digital service providers must notify, without undue delay, to the NCA or the CSIRT incidents that have a significant impact on the continuity or provision of the services (Articles 14(3) and 16(3) of the NIS Directive).

59 As mentioned above, the NIS Directive is not directly applicable in the EU Member States but needs to be implemented in each national Member State law. It can therefore be expected that there will be a

difference in implementation of the security incident notification obligations between the different EU Member States.

2. Notification in Practice

60 The factors to be considered when determining whether the impact of an incident is significant are the following (Articles 14(4) and 16(4) of the NIS Directive):

Operators of essential services	Digital service providers
• the number of users affected by the incident; • the duration of the incident; • and the geographical spread of the incident.	• the number of users affected by the incident; • the duration of the incident; • the geographical spread of the incident; • the extent of the disruption of the service; • and the extent of the impact on economic and societal activities.

Table 3: Factors to determine the significance of an impact

61 In case an operator of essential services depends on a digital service provider for the provision of such essential services, any significant impact on the continuity of those services due to an incident affecting the digital service provider must be notified by that operator (Article 16(5) of the NIS Directive). The NIS Directive remains silent as to whether, in such circumstances, the digital service provider is obliged to notify such an incident to the operator of essential services. It is therefore to be expected (and highly recommended) that the operator of essential services would require such notification by the digital service provider contractually.

62 The notified NCA or CSIRT shall inform other Member States affected (Articles 14(5) and 16(6) of the NIS Directive). In this case, the NCA, the CSIRT, and the single point of contact shall ensure that the service provider's security and commercial interests are safeguarded and that the information provided remains confidential. The NCA or CSIRT may also decide – after consultation of the notifying operator – to inform the public, where such public awareness would be necessary to prevent or manage an incident (Articles 14(6) and 16(7) of the NIS Directive).

3. Sanctions

63 Essential or digital service providers that do not comply with the security incident notifications laid down by the national provisions adopted pursuant to the NIS Directive may be subject to a penalty, which is to be determined by each EU Member State at the national level. Pursuant to Article 21 of the NIS Directive, such penalties must be effective, proportionate and dissuasive.

IV. Conclusion

64 It is highly recommended for big data service providers to document the legal notification requirements applicable to them in a detailed manner, both at the EU and national level, in order to be able to comply with their notification obligations.

65 Big data service providers shall notify any security and/or data breach, which (i) has led to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored, or otherwise processed; or (ii) may lead to a significant disruptive effect on the service provided by themselves or by their customers.

C. Internal Security Strategy

66 The question arises how big data service providers should fit the security and breach notification legal requirements examined in this paper within their internal security strategies.

67 Fig. 3 aims to provide some guidance in this respect. It sets out some of the main aspects to consider at each phase of the incident lifecycle: *i.e.*, pre-incident, during or immediately after the incident, and post-incident. For each phase, Fig. 3 recommends which practical steps to take in order to comply with the legal requirements examined in this paper.

68 Inevitably, an internal incident handling strategy like the one depicted in Fig. 3 can only achieve its purpose if it is constantly re-evaluated and updated in light of the changing circumstances and the new technological abilities. This goes hand in hand with the fact that the legal, statutory, and contractual requirements must be assessed and re-assessed at each step of each phase, in order to ensure full compliance.

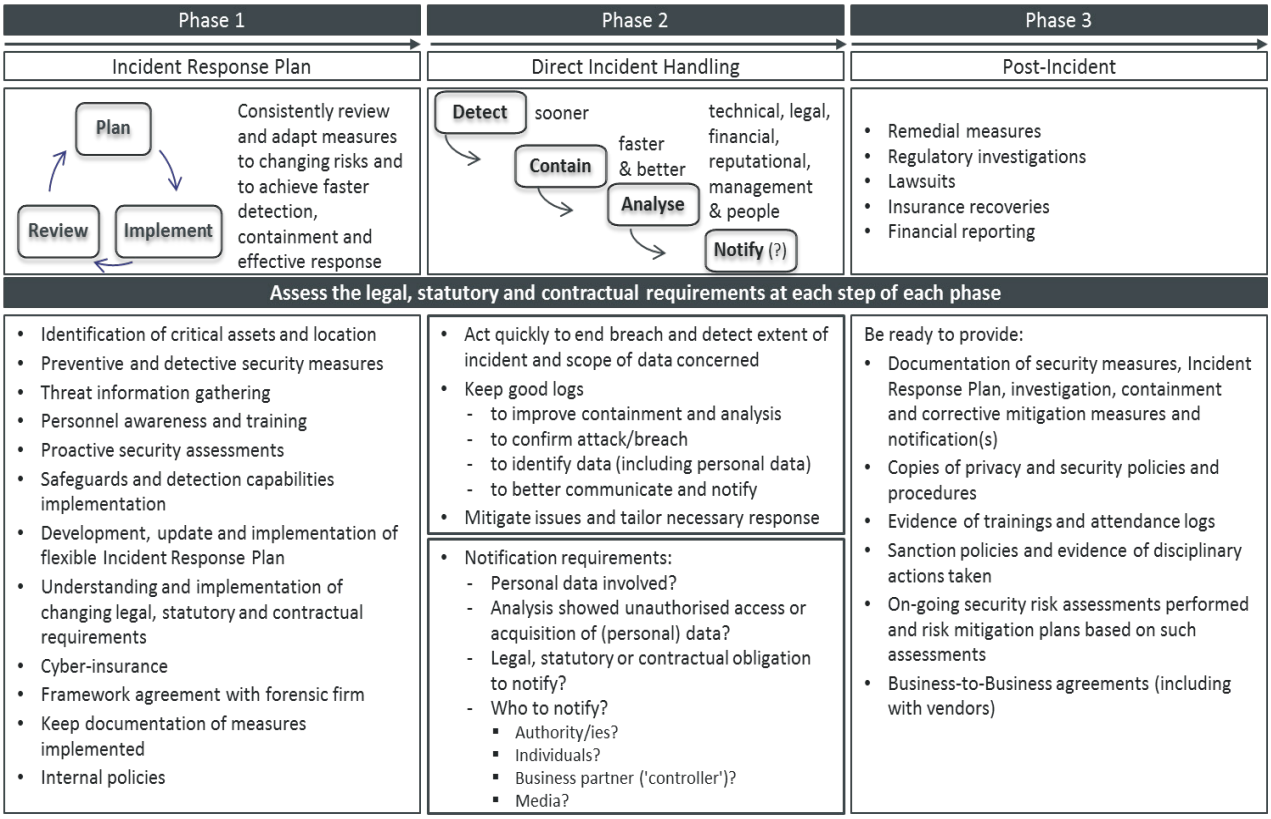

Figure 3: Incident Handling Diagram

References

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a thriving data-driven economy", 2 July 2014, COM(2014) 442 final.

[2] R Naydenov, D. Liveri, L. Dupre, E. Chalvatzi and C. Skouloudi, "Big data security - good practices and recommendations on the security of big data systems", (ENISA 2015).

[3] OECD, "Data-driven innovation: big data for growth and well-being", (OECD Publishing 2015), <http://dx.doi.org/10.1787/9789264229358-en>

[4] MR Overly, "Information security in vendor and business partner relationships" in JR Kalyvas and MR Overly (eds.), *Big Data: A Business and Legal Guide* (Auerbach Publications 2015).

[5] E Damiani, C. A. Ardagna, F. Zavatarelli, E. Rekleitis (ed.) and L. Marinos, "Big data threat landscape and good practice guide", (ENISA 2016).

[6] E Damiani, "Toward big data risk analysis", IEEE International Conference on Big Data (IEEE 2015), Santa Clara, CA, pp. 1905-1909.

[7] J. Ghent, "Digital risk management and data protection", (Innovation value institute, 2014)

[8] Desai, "Law and technology. Beyond location: data security in the 21st century", Communications of the ACM, vol. 56, pp. 34-36, January 2013, doi: 10.1145/2398356.2398368

[9] N. van Dijk, R. Gellert and K. Rommetveit, "A risk to a right? Beyond data protection risk assessments", Computer Law & Security Review: The International Journal of Technology Law and Practice (2015), doi: 10.1016/j.clsr.2015.12.017

[10] Kung and others, "PRIPARE: a new vision on engineering privac and security by design" (2014)

[11] Samaras, S. Daskapan, R. Ahmad and S. Ray, "An enterprise security architecture for accessing SaaS cloud services with BYOD" (2014), doi: 10.1109/ATNAC.2014.7020886

[12] Kosta and K. Stuurman, "Technical standards and the draft General Data Protection Regulation" in P. Delimatsis (ed), *The law, economics and politics of international standardization* (Cambridge University Press, 2016, forthcoming)

[13] Kennedy and C. Millard, "Data security and multi-factor authentication: analysis of requirements under EU law and in selected EU Member States" (2015)

[14] M. Dekker, D. Liveri and M. Lakka, "Cloud Security Incident Reporting – Framework for reporting about major cloud security incidents", (ENISA 2013)

[15] M. Dekker and D. Liveri, "Cloud Security Guide for SMEs – Cloud computing security risks and opportunities for SMEs", (ENISA 2015)

[16] Rijmen, D. De Cock, N. P. Smart and R. Tirtea, "Recommended cryptographic measures – Securing personal data", (ENISA 2013)

[17] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

[18] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1

[19] ISO/IEC 27000:2016 – Information technology, security techniques

* A data controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; a data processor is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller (Article 4 of the GDPR).

This paper was written within the European Union TOREADOR project ("TrustwOrthy model-awaRE Analytics Data platfORm"). Granting authority: European Union. Call: H2020-ICT-2015. Topic: ICT-16-2015 (Big data - research). Type of action: RIA. Grant agreement no.: 688797, Starting date: 1st January 2016, Ending date: 31st December 2018.

Angela Daly, Private Power, Online Information Flows and EU Law: Mind the Gap

Hart Publishing 2016, 184 pages, ISBN 978-1-50990-063-3

Book Review

by **W. Gregory Voss**, Professor of Business Law, Université de Toulouse, Toulouse Business School (TBS), Toulouse

Recommended citation: , W. Gregory Voss, Book Review: Angela Daly, Private Power, Online Information Flows and EU Law: Mind the Gap, 8 (2017) JIPITEC 89 para 1.

1 This book, which is part of the Hart Studies in Competition Law series, may, at first glance, seem to fall outside the scope of the main areas of interest for many scholars in intellectual property, information technology, and e-commerce law. However, the European Commission's issuance of a Statement of Objections to Google regarding comparative shopping services, the opening of a formal competition law investigation into Google's conduct related to the Android mobile operating system, both in 2015, followed by a 2016 report of the French and German competition authorities on competition law and the collection and use of data, should have put an end to any doubt about the interest of competition law to the sectors such scholars study. Furthermore, this book's subject matter is not limited to competition law and concerns European Union telecommunications regulation, privacy and data protection law, the right to free expression, and technical measures intended to limit the impact of concentrations of private economic power on online information flows as well.

2 The first chapter of the book provides an introduction, sets out the mission of the book and outlines its structure and approach. The second chapter establishes the book's theoretical framework which serves as the basis for the discussions of what Daly calls the 'substantive' part of the book, consisting of discrete 'case studies' and providing examples of existing EU law. The first of these is contained in chapter three on dominance and internet provision, particularly covering net neutrality. In the fourth chapter, dominance and internet search are the subject, focussing as might be expected on Google. The fifth chapter deals with dominance and mobile devices, placing an emphasis on application (or 'app') stores. The last of the 'substantive' chapters is chapter six, which covers dominance and the cloud, followed by a conclusion (chapter seven). Notably, each of the substantive chapters contains a competition law analysis, followed by a discussion of other areas of law (data protection and privacy, free expression, etc.) and technique. The chapters are fairly well balanced in terms of length, with the sixth chapter on the cloud being the shortest of the 'substantive' chapters, likely because of its 'speculative' nature, and the fourth chapter on internet search being slightly longer than the theoretical chapter (chapter two) and the chapter on mobile devices (chapter six), due to the European Commission's investigations in this area.

3 In the first chapter, Daly sets out some of the limits of the book. First, it does not cover state-only control of online information flows, such as for the prevention of crime. Second, only current EU law (including the European Convention on Human Rights, as amended) is discussed in detail, to the exclusion of 'possible conceptual reforms'. Finally,

consumer protection law is largely left uncovered by the work, which may disappoint certain readers. The book's main argument is made explicit before being developed in the next and following chapters: "that existing EU law and regulation does not adequately address concentrations of private economic power adversely affecting online information flows to the detriment of Internet users' autonomy due to their neoliberal basis".

4 The second chapter of the book is the most dense and theoretical of all. Daly begins by tracing the history of the Internet from its ARPANET origins, early Internet legislation, the advent of Web 2.0, and the assertion of political and legal control over the medium, the "privatisation" of the same, and the emergence of concentrated private power in the hands of large Internet corporations often operating as "web-based platforms". The book then introduces concepts such as digital labour, economic surveillance, and "the invisible handshake" between states and large online players (i.e. the collaboration between states and large Internet corporations, which usually escapes public awareness), with platforms taking a role in policing online activity which falls afoul of copyright and other laws. "User autonomy" (as preferred to "consumer welfare") is pictured as a desirable goal for EU law and regulation, with 'users' being described as individuals "who both produce and consume information over the internet", thus distinguishing them from mere consumers – "an inappropriate and outdated concept given the increased capacity for individuals to produce as well as consume facilitated by the internet", according to Daly. This implies optimal online information flows, without censorship, "illegitimate" restrictions or blanket surveillance.

5 Daly then points to what she views as different shortcomings of competition law (and of the arguments of the influential Chicago School) in the context of the Internet. This is due in part to it not being well adapted to free goods and its focus on consumer welfare as opposed to user autonomy, which she argues does not account for new needs and desires of users, such as the production of content. She rightly identifies two recent factors – the development of Big Data and the entry into force of the EU Charter of Fundamental Rights (covering rights to protection of private life, protection of personal data, freedom of expression and information, etc) – as having shifted the debate on competition law and social/non-economic factors (such as human rights). The EDPS is cited in this context taking the view that it may be necessary to incorporate data protection violations into the concept of consumer harms for competition law enforcement purposes. However, Daly aptly points out that such non-economic factors of user autonomy may conflict with neo-liberalism and cause regulatory tension for competition authorities. Unfortunately, Daly avoids discussing potential paths of competition law reform here as it is outside the scope of her book. However, she does point to "regulatory capture", which may result from corporate lobbying and the time lag for regulation as factors which may force users to seek alternative ways to advance autonomy, such as 'code-based' technical solutions.

6 Dominance in the context of Internet provision is covered by the first of Daly's case studies in the third chapter centred on ISPs – the only such study where ex-ante regulation has been adopted. Here a very helpful and clear explanation of net neutrality has been provided in the context of the concentration of Internet content in large players that can afford to use content delivery networks (CDNs) and/or make deals with Internet access providers to achieve more favourable results (such as speedy provision of their data to users) for themselves. As in the other case studies, the focus is on a 'choke-point' of the Internet, where an information gate-keeper (here, the ISP) is placed. Without specifying the myriad details of this chapter, it is important to highlight the role of deep packet inspection (DPI) technology, which allows ISPs to use their power to control what data their customers could access. This raises concerns with regards to competition law, especially where ISPs have a dominant position in their market or 'significant market power'. In addition, there is a perceived invasion of privacy tied to the use of DPI. Sector-specific (telecommunications) regulation and competition law already exist in the EU to cover this area, and these are supplemented by data protection and privacy laws, however national security exceptions may apply. Otherwise, ISPs are prohibited from "listening, trapping, storage or other kinds of interception or surveillance of communications" without users' consent under the ePrivacy Directive, unless an exception applies, however it may be difficult to obtain knowledge that a violation exists. Daly points to weaknesses in the Net Neutrality Regulation, as a measure that came "too little, too late" when technology and business practice have moved on, specifically highlighting that it would be difficult today to ban CDNs because of their widespread use. What may be left are technical solutions such as the use of encryption technology to block ISPs from monitoring the content of data, and other solutions such as P2P file-sharing networks and community mesh networks, each with its own weaknesses.

7 In the fourth chapter, dominance in Internet search is the focus – arguably the most currently visible of the areas from a competition law perspective, with the dominant search engine Google in the European regulator's spotlight. The importance of search engines for the finding of information and making sense of it on the Internet goes without saying,

although competition law only addresses economic concerns in this regard and not non-economic ones such as biased information-filtering privacy and data protection infringements according to Daly. Relevant to the Google cases, the creation of barriers to entry may result in the field of online search and advertising from the collection of information about users and their behaviour by the search engine. As search engines are not subject to any sector-specific ex-ante regulation in the EU (unlike ISPs), Daly informs us that the initial legal solution for problems in this area is to be found in competition law, and application of such law is made easier because of Google's dominant position in online search and advertising. Daly reminds us of the information asymmetry due to the opacity of Google's algorithm – a subject that could have been explored in further detail by the author. In this chapter, the author also studies the various elements of the European Commission's investigation into Google (involving, inter alia, favouring its own comparison shopping service in search results) and prior cases involving the giant, as well as highlighting its role in the "invisible handshake" with the US authorities unveiled by the Snowden NSA revelations. Daly suggests that further regulatory reform, potentially involving transparency and "search neutrality", may be desirable, and that extra-legal solutions such as the creation of alternative search solutions either through state action or through peer-to-peer design are suggested as a potential way forward. However, it remains to be seen whether these are realistic options given the failure of past initiatives such as the Quaero case that Daly mentions.

8 Next, dominance and mobile devices are covered by the author in the fifth chapter. Here a focus has been on the vertical integration of closed systems, with power being concentrated through app stores. Problems related to anticompetitive conduct by the entities controlling the app stores, to expression and control (censorship or limitations placed on what you can do with devices), and to privacy and data protection of user data, are highlighted. From a technical standpoint, digital rights management measures (DRMs) and technical protected measures (TPMs) may be used to effectively lock users into an app store or system. However, here one hurdle is that there is no dominant player who might be subject to an abuse of a dominant position claim in the broader market, although a specific app store may constitute a market in and of itself, depending on the facts. Daly discusses cases involving Apple and Google on e-books, Google Play, then Android in this context, as well as potential anti-competitive conduct such as tying, locking users into an ecosystem, and blocking apps. The author sees the right to data portability, contained in the forthcoming EU General Data Protection Regulation (GDPR), as a potential tool, but cautions that it only applies to data processing for which the legitimate basis is consent (or a contract). Once again, Daly finds gaps relevant to user autonomy in existing legislation and regulation.

9 The last of Daly's cases studies – one covering dominance and the cloud – is contained in the sixth chapter and is, according to her, the more "speculative" chapter as it addresses cloud services before they have been subject to any competition investigation. After describing the different kinds of clouds, the book sets out perceived problems with the cloud. One such issue involves DRMs and TPMs in the cloud, which may be more restrictive than what the law requires, where the original goal of such measures was protection of the rights of copyright owners, and where permitted user exceptions are not considered for use in the cloud, the result being a lack of portability and interoperability for users. In addition, network effects and associated accumulation of user data by platforms may create a barrier to entry. Nonetheless, Daly considers that the markets for cloud appear quite competitive and that it would be difficult to find dominance or collusion, such as to allow the use of competition law to curtail anti-competitive behaviour that limits users' autonomy.

10 The conclusion of the book revisits some of the arguments detailed above, reminding the reader of some of the limitations of the work, and positing that areas for future research include a "more thorough consideration of consumer protection's role in advancing user autonomy online"; in particular, potential conceptual reform of the area to take consumer protection law to "prosumer" protection law, taking into consideration the productive attribute of users as well. Daly concludes that technical measures may be the "most realistic" way for users to protect their autonomy online.

11 This discussion of the importance of technical measures, together with an elucidation of the difficulties of competition law within the online context in the absence of findings of dominance, constitute strong points of the book, along with a very helpful explanation of net neutrality provided at a moment when the new US administration is calling this principle into question. The organisation of chapters following the development of the theoretical framework around the "substantive" cases of ISPs, search, mobile devices, and the cloud, is effective for the purposes of the study. The analysis focussed on neoliberalism is interesting, as is the critique of some of the European Union's regulatory approach (chapter two); nonetheless, some of the author's choices of language, such as "Big Data evangelists" and "technocorporatist alliance" (chapter 5) might be considered by some readers as unfortunate, however sympathetic they may be with Daly's arguments. One detailed point

might be made in order to provide clarity for the readers, although this takes nothing away from the author's arguments: in chapter six Daly refers to article 3 of the GDPR as providing that the regulation applies to "controllers or processors not established within the EU but which are processing EU citizens' data"; yet, article 3(2) of the GDPR imposes no such requirement of EU citizenship, and refers instead to "the processing of personal data of data subjects who are in the Union" in connection with the offer of goods or services (including "free" ones) to them, or the monitoring of their behaviour to the extent that it occurs in the Union.

12 As discussed above, the reader may have hoped that this book contained suggestions for competition law reform to address the gaps Daly has identified, or a greater handling of consumer protection law and the discussion around digital labour, or even a further development covering the interplay between competition law and intellectual property in the online context. The author would have rightly argued lack of space; moreover, she does provide solutions which are alternatives to competition law in regulating private power and does posit "user autonomy" as a goal to be preferred over "consumer welfare". Notwithstanding such gaps, Daly's very readable book provides an important and well-researched contribution in an area – competition law – that is now inextricably linked to the domains of other legal specialties such as privacy and data protection, the right of expression, and intellectual property. Thus, this book is highly recommended reading for Internet scholars, whatever their specific area of expertise.

jipitec

Journal of
Intellectual Property,
Information Technology,
and Electronic Commerce
Law

www.jipitec.eu