German Law Journal (2019), **20**, pp. 679–721
doi:10.1017/glj.2019.56

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Pre-formulated Declarations of Data Subject Consent—Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections

Damian Clifford*, Inge Graef** and Peggy Valcke***

(Received 21 February 2018; accepted 16 July 2018)

Abstract
One of the novelties brought about by the new General Data Protection Regulation (GDPR) is a strengthening of the concept of consent. For instance, although the freely given stipulation existed in the old framework—the Data Protection Directive 95/46/EC—the changes introduced by the GDPR arguably imply that access to services may no longer depend on data subject consent. In reality however, data subjects often find themselves confronted with standard privacy policies and take-it-or-leave-it offers. Against this background, this Article aims to examine the alignment of the respective data protection and privacy, consumer protection, and competition law policy agendas through the lens of pre-formulated declarations of consent. The Article aims to delineate the role of each area with specific reference to the GDPR and ePrivacy Directive, the Unfair Terms Directive, the Consumer Rights Directive, and the Digital Content Directive (Compromise), in addition to market dominance. Competition law analysis is explored vis-à-vis whether it could offer indicators of when a clear imbalance in controller-data subject relations may occur in the context of the requirement for consent to be freely given, as per its definition in the GDPR. This complements the data protection and consumer protection analysis which focuses on the specific reference to the Unfair Terms Directive in Recital 42 GDPR, stating that pre-formulated declarations of consent should not contain unfair terms.

Keywords: Consent; personal data; unfair terms; market dominance

A. Introduction

In the Information Society Services (ISS) context, pre-formulated privacy policies and terms of use are the norm, largely due to practical realities. Given the detailed information communicated to the user—or data subject in the data protection law nomenclature—standard form texts are a necessity. There have, however, been several high-profile examples of how such policies can be used to disadvantage data subjects. From the inclusion of publicity stunt clauses—such as

*Researcher (FWO Aspirant Fellow), KU Leuven CiTiP Sint-Michielsstraat 6, box 3443 3000 Leuven (Belgium), +32 16 37 62 11, damian.clifford@kuleuven.be.
**Assistant Professor Tilburg University, TILT & TILEC, PO Box 90153 5000 LE Tilburg (The Netherlands), +31 13 466 8758, i.graef@tilburguniversity.edu.
***Research Professor KU Leuven CiTiP Sint-Michielsstraat 6, box 3443 3000 Leuven (Belgium), +32 16 32 54 70, peggy.valcke@kuleuven.be.

© 2019 The Author. Published by Cambridge University Press on behalf of the *German Law Journal*. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits unrestricted reuse, distribution, and reproduction in any medium, provided the original work is properly cited.

المنارة للاستشارات
www.

the requirement to surrender your first-born child[1] or to clean the city sewers[2]—to the more practical everyday problems associated with the complex legalese and lengthy texts found in such documents,[3] privacy policies are an easy target for critics given their apparent futility in their primary function, namely, informing data subjects on how their personal data are processed. Other authors, however, have defended the use of privacy policies referencing the need for such mechanisms and their role in informing not only data subjects, but also inter alia enforcement agencies, civil society, and academia.[4] Clearly, privacy policies are designed for more than individual data subjects. Accordingly, despite the fact that there are clear issues, criticism placed against privacy policies should be nuanced.

The above examples highlight the ongoing concerns regarding the legitimacy of data subject consent to the processing of personal data that is based on pre-formulated privacy policies. With the reform of the data protection framework and the entry into force of the General Data Protection Regulation (GDPR),[5] the EU legislator has aimed to address these issues. As illustrated elsewhere, the GDPR has arguably emphasized the significance of the fairness principle.[6] This principle plays an important role in the strengthening of data subject consent both internally within the operation of the GDPR, and externally, via a reference to the alignment and concurrent application of the consumer protection framework. The cross-reference to the Unfair Terms Directive (UCT Directive) in Recital 42 of the GDPR raises a number of questions vis-à-vis the precise nature of the relationship between these data protection and consumer protection frameworks, which are part of distinct policy agendas. In addition, Recital 42 GDPR refers specifically to pre-formulated declarations of consent, thereby raising key questions regarding the overlaps between such pre-formulated declarations, privacy policies, terms of use, and contract law more generally. The confusion in relation to the overlaps between contract and consent as conditions for the lawful processing of personal data is an illustration of the challenge associated with this policy agenda interplay. In this regard, one can refer to the most recent action taken by the activist Max Schrems against Google, Instagram, WhatsApp, and Facebook regarding these companies' consent-bundling practices and take-it-or-leave-it requests for consent.[7] These practices illustrate that, although consumers are given ever stronger protections in legislative instruments, including the GDPR, practice shows that it remains difficult to effectively enforce these protections against digital giants. One of the complexities in this regard is how to apply different legal regimes based on distinct policy agendas in parallel.

The objective of the Article, therefore, is to elucidate the key divergences between data and consumer protection with reference to the overlap between the GDPR and the UCT Directive to highlight the fundamental difficulties associated with the alignment of protections. Building on this analysis, the role of competition law will be examined. In particular, the inherent asymmetries associated with the practical implementation of pre-formulated declarations of

[1]Leyden John, *Consumers Agree to Give up First-Born Child for Free Wi-Fi—Survey*, The Register (September 30, 2014), https://www.theregister.co.uk/2014/09/30/free_wi_fi_survey.

[2]Alex Hern, *Thousands Sign up to Clean Sewage Because They Didn't Read the Small Print*, The Guardian (July 14, 2017), http://www.theguardian.com/technology/2017/jul/14/wifi-terms-and-conditions-thousands-sign-up-clean-sewage-did-not-read-small-print.

[3]The Norwegian consumer authority live-streamed the reading of the terms of smartphone applications. *See Norway Stages 32-Hour App Term Reading*, BBC News (May 25, 2016), http://www.bbc.co.uk/news/world-europe-36378215.

[4]*See* Mike Hintze, *In Defense of the Long Privacy Statement*, 76 Md. L. Rev. 1044 (2016); Mike Hintze, *Privacy Statements*, *in* The Cambridge Handbook of Consumer Privacy 413 (Evan Selinger et al. eds., 2018).

[5]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 [hereinafter GDPR].

[6]Damian Clifford & Jef Ausloos, *Data Protection and the Role of Fairness*, 37 Y.B. of Eur. L. 137 (2018).

[7]Rebecca Hill, *Max Schrems Is Back: Facebook, Google Hit with GDPR Complaint*, The Register (May 25, 2018), https://www.theregister.co.uk/2018/05/25/schrems_is_back_facebook_google_get_served_gdpr_complaint; Derek Scally, *Max Schrems Files First Cases under GDPR against Facebook and Google*, The Irish Times (May 25, 2018), https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177

المنارة للاستشارات
www.

consent and take-it-or-leave-it choices arguably point to the relevance of competition law analysis as a mechanism to ensure the availability of choice—as opposed to the protection of the ability to choose safeguarded by the consumer and data protection frameworks.

The methodology relies on a legal analysis of how the alignment of the data and consumer protection frameworks challenges the existing paradigms associated with the respective policy agendas in aiming to counteract the inherent data subject-controller asymmetries and the extent to which competition law analysis may contribute to the application of protections. The legal instruments have been selected on the basis of their substantive and material scope. Section B of the Article will explore the role of fairness in data protection, introduce the cross-reference to the UCT Directive, and position the broader debate. Section C of the Article aims to differentiate pre-formulated from individual negotiated terms with reference to the UCT Directive and case law. Section D explores the notion of core terms, whether the provision of personal data can be classified as such—and thus be attributed an economic value—, and the effects of these considerations on the separation between pre-formulated declarations, privacy policies, and terms of use as three distinct but overlapping notions. Building on this, the final Section of the Article will explore what is meant by freely given consent in more detail with reference to competition law analysis.

B. Aligned Citizen-Consumer Protections—Effectuating Meaningful Choice

The introduction of the Lisbon Treaty was a watershed moment for the protection of the fundamental right to data protection. Through the adoption of the Lisbon Treaty, the Charter of Fundamental Rights of the European Union (the Charter) was given binding force, and, as a result, the right to data protection was recognized as a distinct right for the first time.[8] The GDPR, as a secondary framework adopted under Article 16 TFEU, which provides a basis for the EU to adopt legislation for the protection of the right to data protection, further specifies the operation and protection of the right to data protection in particular, and rights and freedoms more generally when personal data are processed.[9] Personal data are as "any information relating to an identified or identifiable natural person ("data subject")."[10] When combined with the definition of pseudonymization[11] and the clarification regarding the interaction between these two definitions,[12] it is apparent that the personal data definition encompasses any data capable of singling out an individual.[13] A controller is defined as the natural or legal person "which, alone or jointly with others, determines the purposes and means of the processing of personal data"[14] and, a processor, as any natural or legal person "which processes personal data on behalf of the controller."[15]

[8]Although the European Court of Human Rights has interpreted the protection of personal data as part of the right to respect for private and family life—for example, as provided for in Article 8 of the European Convention of Human Rights—the Charter delineates data protection—Article 8 Charter—and privacy—Article 7 Charter—thereby recognizing them as independent rights in EU law. *See* S & Marper v. United Kingdom, App. Nos. 30562/04 and 30566/04 (2008).

[9]*See* GDPR, *supra* 5, at art. 1(2).

[10]*Id.* at art. 4(1).

[11]*See id.* at art. 4(5).

[12]*See id.* at recitals 26, 28.

[13]*See* Frederik J. Zuiderveen Borgesius, *Singling out People without Knowing Their Names—Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation*, 32 Computer L. & Security Rev. 256 (2016), http://www.sciencedirect.com/science/article/pii/S0267364915001788. This clarification should be recognized as a significant take-away, given that a failure to include such data within the scope of the definition of personal data would have undermined the protections provided by the framework. Indeed, the capacity to single out raises the need for protection irrespective of whether one can identify an individual's name. *See* Damian Clifford & Valerie Verdoodt, *Integrative Advertising: The Marketing "Dark Side" or Merely the Emperor's New Clothes?*, 8 Eur. J. of L. and Tech. (2017), http://ejlt.org/article/view/547.

[14]*See* GDPR, *supra* 5, at art. 4(7).

[15]*See* GDPR, *supra* 5, at art. 4(8).

المنارة للاستشارات
www.

The data protection framework is designed to counteract power and information asymmetries between controllers, processors, and data subjects, and to strengthen the position of data subjects relative to controllers.[16] In doing so, the framework attributes rights to data subjects and obligations to controllers—and processers—and provides for a clear separation in responsibilities with controllers processing data subjects' personal data—with or without contracting the services of a processor, who hold merely a passive function—and with each entity easily distinguishable within the framework.[17] But, the suitability of the data protection framework has been repeatedly questioned given the emergence of the so-called big data environment and the datafication of everything.[18]

I. The GDPR, Fairness, and the Regulatory Response to Technological Development

Key data protection principles such, as inter alia, data minimization, purpose limitation, security and confidentiality, and accuracy are all arguably problematic in terms of practical application.[19] Such criticism has manifested itself clearly in terms of the positioning of informational self-determination and control as a key rationale for the protection provided by the framework. This reflects the questions surrounding the capacity of data subjects to act in their own best interests and make autonomous decisions given the inherent power asymmetries in the data subject-controller relationship. In response to these concerns, the data protection framework has recently been reformed. Although the GDPR largely upholds the traditional regulatory approach, which was evident in Directive 95/46/EC,[20] there have been some notable developments in response to the rapid technological change. More specifically, the GDPR has explicitly introduced the principles of accountability and transparency—the notion of data protection by design and default—and moved towards a risk-based approach. As illustrated in Figure 1 below, there is a clear focus on accountability and transparency in Article 5 GDPR. Indeed, although both the accountability and transparency principles had implicitly played a role in the Directive 95/46/EC, this is the first time that these principles have been expressly provided for in an EU data protection legislative text. Moreover, although risk has always been important in data protection, the GDPR is an example of a risk-based legislative framework in that it places risk at its operative center, thereby affecting the interpretation of all rights and obligations contained therein.[21]

These additions accentuate the importance of the fairness principle.[22] More specifically, given that the GDPR is an example of decentered regulation—namely by placing controllers in charge of how they comply and thus balance fundamentals and interests when personal data are processed—there is increased reliance on risk and accountability and, as a corollary, the obligation for controllers to process personal data fairly.[23]

[16]Orla Lynskey, *Deconstructing Data Protection: The "Added-Value" Of A Right To Data Protection In The EU Legal Order*, 63 Int'l & Comp. L.Q. 569, 563 (2014).

[17]Damian Clifford, '*EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster—Tracking the Crumbs of Online User Behaviour*', 5 JIPITEC (2014), https://www.jipitec.eu/issues/jipitec-5-3-2014/4095.

[18]*See generally* Viktor Mayer-Schonberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work and Think (Houghton Mifflin Harcourt, 2013).

[19]*See generally* Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 Seton Hall L. Rev. 2 (2017); Mireille Hildebrandt et al., *On Decision Transparency, or How to Enhance Data Protection after the Computational Turn*, *in* Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology 196 (Routledge, 2013); Bert-Jaap Koops, *The Trouble with European Data Protection Law*, 4 Int'l Data Privacy L. 250 (2014); Paul De Hert & Vagelis Papakonstantinou, *The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals*, 28 Computer L. & Security Rev. 130 (2012).

[20]De Hert & Papakonstantinou, *supra* note 19.

[21]Article 29 Working Party, *Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks* (May 30, 2014) WP 218; Claudia Quelle, *The "Risk Revolution" in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too*, *in* Data Protection and Privacy: The Age of Intelligent Machines (Ronald Leenes et al. eds., 2017).

[22]Clifford, *supra* note 6.

[23]*Id.*

المنارة للاستشارات
www.

THE PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA			
ARTICLE		**PRINCIPLE(S)**	**RELEVANT EXTRACT FROM PROVISION**
Article 5(1)	(a)	Lawfulness, fairness and transparency	Personal data shall be: processed lawfully, fairly and in a transparent manner in relation to the data subject
	(b)	Purpose limitation	collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes
	(c)	Data minimisation	Personal data shall be: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
	(d)	Accuracy	Personal data shall be: accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
	(e)	Storage limitation	Personal data shall be: kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed...
	(f)	Integrity and confidentiality	Personal data shall be: processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Article 5(2)		Accountability	The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1

Figure 1.

Although fairness has long been positioned as a key tenet of data protection law, it appears to have gained increased significance in the GDPR. As argued more extensively elsewhere, the fairness principle can be divided into two key elements, namely: Procedural fairness and fair balancing. Each of these elements is then made up of specific components, as illustrated in Figure 2 below.[24]

In simple terms, both elements will run concurrently in the context of any given processing operation. Essentially, the elements manifest themselves in the balancing of rights and interests and mandate that controllers must take the rights and interests of data subjects into account—or in other words, not "ride roughshod" over the wishes of the latter.[25] The fairness principle also requires controllers to ensure that data subjects are informed and capable of exercising their right to data protection—thereby seemingly burdening controllers with an obligation to be mindful of data subject's interests and capacities. This role for the fairness principle is manifested in *ex ante* and *ex post* fair balancing and procedural fairness safeguards which are evident throughout the provisions of the GDPR. The *ex ante* application of the fairness principle here refers to the rights and obligations which apply prior to personal data processing—the application of the conditions for lawful processing in Article 6(1) GDPR, for example—whereas the *ex post* safeguards relate to the rights and obligations which apply during personal data processing—like the application of data subject rights.

In this manner, the GDPR, as a secondary framework designed to protect rights and freedoms and the right to data protection in particular,[26] aims to satisfy the requirements for the limitation

[24] *Id.*

[25] LEE A BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS 58 (The Hague Kluwer Law International, 2002).

[26] *See* GDPR, *supra* 5, at art. 1(2).

المنارة للاستشارات
www.

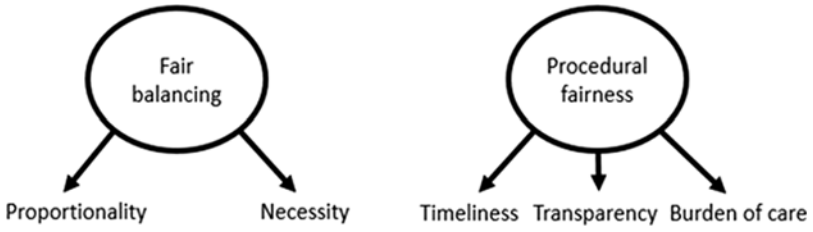

Figure 2.

of rights in Article 52(1) of the Charter, read in conjunction with Article 8(2) of Charter as outlined above. Article 52(1) of the Charter specifies that:

> [A]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be *provided for by law* and *respect the essence of those rights and freedoms*. Subject to the *principle of proportionality*, limitations may be made only if they are *necessary and genuinely meet objectives of general interest* recognised by the Union or the need to protect the rights and freedoms of others.[27]

Therefore, the GDPR is a secondary framework based on fairness checks and balances which aims to balance competing rights and interests in line with this proportionality and necessity test in Article 52(1) of the Charter where personal data are processed. As mentioned above, in the pursuit of this objective, the fairness principle transverses the entire operation of the framework. To clarify, in an *ex ante* sense, the processing of personal data requires one of the conditions for lawful processing contained in Article 6(1) GDPR to be satisfied. Regarding the provision of ISS, three of these conditions are specifically relevant, namely: Consent,[28] contract,[29] and legitimate interests,[30] as represented below in Figure 3.[31]

The purpose of the processing, the means used to achieve this purpose, and the interests at stake will determine which of these conditions may be applicable. Consequently, each of the three conditions—as with the other conditions in Article 6(1) GDPR—plays a distinct and delineated role.[32] Importantly, the Article 29 Working Party[33] has observed that where large amounts of personal data are collected in a commercial setting, consent will often be the only appropriate condition.[34] The fairness principle is key in the operation of each of these conditions.

II. Consent, Unfair Terms, and Fair Personal Data Processing

Although consent has always been important to the operation of the data protection framework—being specifically mentioned in Article 8(2) of the Charter—reliance on this condition as a

[27]Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community art. 52(1), Dec. 13, 2007, 2007 O.J. (C 306) (emphasis added) [hereinafter The Charter].

[28]*See* GDPR, *supra* 5, at art. 6(1)(a).

[29]*Id.* at art. 6(1)(b).

[30]*Id.* at art. 6(1)(f).

[31]Importantly, in this context, commercial activities exclude processing that is necessary for compliance with a legal obligation as laid down in Article 6(1)(c) of the GDPR.

[32]For a description of the operation of each of these conditions for lawful processing, see Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC*, WP 217 (Apr. 9, 2014).

[33]Now the European Data Protection Board; references to the Article 29 Working Party, however, will be maintained in this Article in order to avoid unnecessary confusion for readers given that the opinions referenced refer to the Working Party.

[34]*See* Opinion 06/2014, *supra* 32; Article 29 Data Protection Working Party, *Opinion 02/2010 on Online Behavioural Advertising*, WP 171 (June 22, 2010).

المنارة للاستشارات
www.

LAWFULNESS OF PROCESSING		
ARTICLE	CONDITION	RELEVANT EXTRACT FROM PROVISION
Article 6(1)(a)	Consent	the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
Article 6(1)(b)	Contract	processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
Article 6(1)(f)	Legitimate interest	processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Figure 3.

meaningful means of legitimizing personal data processing has been repeatedly questioned. In short, bounded data subject rationality and the cognitive biases exposed by behavioral economics research have undermined the value of a reliance on consent in relation to its correlation to the data subject true wishes and understandings.[35] More specifically, the multiplicity of requests for consent and the resulting apparent dilution of its importance, the stickiness of default settings, market effects including lock-in, the complex legalese evident in privacy policies, and information overload have seemingly undermined the value of data subject participation and rendered consent increasingly difficult to apply in practice.[36] In response to these issues, the EU legislator has strengthened consent in the GDPR, thereby recognizing an increased role for the controller in ensuring the legitimacy of this condition for lawful processing.

Consent is defined in Article 4(11) GDPR as "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."[37] Articles 4(11) and 6(1)(a) GDPR, in Figure 3 above, are then further specified in the conditions for consent in Article 7 GDPR, as represented below in Figure 4.

Article 7 GDPR is a key GDPR innovation designed to empower data subjects. Although the operation of Article 7 GDPR will be explored in detail later, for our current purposes, it is important to highlight how this provision manifests the application of the fairness principle. In particular, Article 7 GDPR appears to establish a burden of care on controllers regarding their responsibility to ensure that data subjects have been informed and understand the provided information. The controller is required to be able to demonstrate consent,[38] keeping in mind that, in assessing the freely given definitional condition, rendering access to the service conditional on consent may invalidate the reliance on consent.[39]

Moreover, it is the controller's responsibility to take the interests and limitations of data subjects into account vis-à-vis the requirement for specific unambiguous information in line with the transparency principle. This is a direct manifestation of the procedural fairness element—in

[35]Laura Brandimarte & Alessandro Acquisti, *The Economics of Privacy*, *in* THE OXFORD HANDBOOK OF THE DIGITAL ECONOMY (Martin Peitz & Joel Waldfogel eds., 2012); Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*, 4 SOC. PSYCHOL AND PERSONALITY SCI. 340 (2012); Lauren E. Willis, *Why Not Privacy by Default*?, 29 BERKELEY TECH. L. J. (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id%3d2349766.

[36]The readiness of data subjects to consent to the surrender of their personal data without being aware of the specific purpose indicated—or, indeed of the data gathering in the first place—is a good illustration of this point. Despite the fact that reliance on consent as a ground for personal data processing is questionable, a critique well-founded in literature, there is a continuing move towards empowerment at a policy level. *See generally* Clifford, *supra* note 17.

[37]GDPR, *supra* 5, at art. 4(11).

[38]*Id.* at art.7(1).

[39]*Id.* at art. 7(4).

www.

ARTICLE 7 GDPR CONDITIONS FOR CONSENT	
ARTICLE 7(1)	Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
ARTICLE 7(2)	If the data subject's consent is given in the context of a written declaration which also concerns other matters, the 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. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
ARTICLE 7(3)	The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
ARTICLE 7(4)	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.

Figure 4.

other words, controllers are burdened with care. In addition, it should be understood that, in the determination of the legitimacy of consent and thus the operation of the key definitional conditions,[40] there is also a key role for the fair balancing element, and, in particular, the operation of the freely given criterion. Put briefly, consent is supposed to represent a meaningful choice as evidenced by the ability to withdraw consent in Article 7(2) GDPR, but also the separation of contract and consent in Article 7(4) GDPR. In this vein, controllers are required to take the rights and interests of data subjects into consideration in order to ensure that the consent is legitimate.

Therefore, Article 7 GDPR, is a significant addition and has resulted in an intense debate surrounding the suitability of other conditions, namely, Article 6(1)(b) GDPR and Article 6(1)(f) GDPR, to legitimize commercial processing operations. As alluded to in the Introduction, the actions taken by Max Schrems against Google, Instagram, WhatsApp, and Facebook refer to this need for the separation of consent from the processing of personal data necessary for the provision of the service as provided for in Article 7(4) GDPR. Nevertheless, this separation is complicated by the cross-reference to the UCT Directive in Recital 42 GDPR regarding the fairness of pre-formulated declarations of data subject consent. Indeed, in addition to the entirely internalized fairness assessment—through the operation of the GDPR's fairness principle—one must also take the UCT Directive into account. Recital 42 GDPR states that:

> 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*. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.[41] [Emphasis added]

[40]To clarify these are informed, specific, freely given, and unambiguous.
[41]*See* GDPR, *supra* 5, at recital 42.

المنارة للاستشارات
www.

This recital, therefore, makes an explicit cross-reference to consumer protection law and more particularly stipulates the requirement that pre-formulated declarations of consent must respect the protections against unfair contractual terms in the UCT Directive. Similar to the GDPR, the UCT Directive works from the assumption that there is an imbalance in bargaining power between suppliers and consumers, and in essence provides that unfair terms shall not be binding for the consumer.[42] Unfairness under the UCT Directive consists of a substantive element—including good faith and significant imbalance components to be assessed at the national level—and a formal transparency and information provision, as provided for in Articles 3–5 of the Directive.[43] As noted by Donnelly and White, "[a]lthough the first of these mechanisms has inevitably been the more high profile, it is arguable that the primary weighting of Directive 93/13 is toward the latter mechanism."[44] This observation reflects the strongly held national contract law traditions, which will be discussed in Section D, and also the traditional objections to regulatory inference with the notion of freedom of contract.[45]

This cross-reference, however, has arguably muddied the waters between consent and contract due to the reliance on the UCT Directive in relation to pre-formulated declarations of consent when contract is provided for as a distinct condition for personal data processing in Article 6(1)(b) GDPR. In addition, this cross-reference raises questions regarding the precise overlaps between the respective notions of fairness contained in the frameworks, given that the UCT Directive does not have the same fundamental rights foundations as the GDPR. Indeed, in contrast to data protection, which, as noted above, is protected as a distinct fundamental right in Article 8 of the Charter, consumer protection is merely provided for as a principle in Article 38 of the Charter. In simple terms, rights and principles are weighted differently in terms of their significance.[46] As a consequence, plotting the relationship between the GDPR and the UCT Directive is not straightforward. Intuitively, the fact that the GDPR applies in a commercial context denotes that it plays an important role in the protection of consumer interests. But, the fundamental rights foundations of the GDPR brings such a simplistic conclusion into question. As a consequence, precisely mapping the relationship between the UCT Directive, as a specific B2 C framework, and the GDPR, as an omnibus regime designed to protect the fundamental rights of citizens—thereby extending beyond the mere B2 C context—in the protection of citizen-consumers is of key importance. With such apparent distinctions between the two instruments, the analysis now turns to a more substantive discussion of the overlaps.

C. Pre-Formulated Declarations of Consent and the Bits In Between

In the binding provisions of the GDPR, the potential for pre-formulated declarations of consent is not explicitly mentioned. Indeed, although Article 7(2) GDPR refers to the separation of data

[42] *See* Joined Cases C-240/98 to C-244/98, Océano Grupo Editorial SA v. Roció Murciano Quintero and Salvat Editores SA v. José M Sánchez Alcón Prades, José Luis Copano Badillo, Mohammed Berroane and Emilio Viñas Feliú, 2000 E.C.R. I-04941. The Court noted:

> [T]he 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 the terms.

[43] Hans-W Micklitz, *Unfair Terms in Consumer Contracts*, *in* 2 EUR. CONSUMER L. 142 (Hans-W Micklitz et al eds., 2014).

[44] MARY DONNELLY & FIDELMA WHITE, CONSUMER LAW: RIGHTS AND REGULATION 239 (Thomson Round Hall, 2014).

[45] *See Id.* (referring to PATRICK S. ATIYAH, THE RISE AND FALL OF FREEDOM OF CONTRACT (Oxford Univ. Press, 1985)).

[46] Article 38 of The Charter stipulates that "[u]nion policies shall ensure a high level of consumer protection." This distinction is significant as Article 52(1) of The Charter (see above) specifies that any limitation on the exercise of rights is required to be "provided for by law and respect the essence of those rights and freedoms," whereas as per Article 52(5) of The Charter, principles "may be implemented by legislative and executive acts taken by institutions, bodies, offices and agencies of the Union, and by acts of Member States when they are implementing Union Law." In addition, Article 52(5) of the Charter goes on to further specify that principles are only "judicially cognisable" in the interpretation of these acts.

المنارة للاستشارات
www.

subject consent given in the context of a written declaration from the other matters which may be included in such a declaration, like in Figure 4 above, this provision remains neutral in terms of its origin and nature. Instead, Article 7(2) GDPR stipulates more generally that such a written declaration must be presented "in an intelligible and easily accessible form, using clear and plain language."[47] Such an approach is also reflected in Article 12(1) GDPR, which states that:

> [T]he controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a *concise, transparent, intelligible and easily accessible form, using clear and plain language*, in particular for any information addressed specifically to a child. *The information shall be provided in writing, or by other means, including, where appropriate, by electronic means*. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.[48]

Hence, Article 12(1) GDPR also has a wider scope of application than merely pre-formulated declarations, as evidenced by the use of the words "or by other means."[49] That being said, such mechanisms are certainly included within its scope. As clarified in the previous Section, although the GDPR's binding provisions do not delineate between boilerplate and individually negotiated declarations, Recital 42 GDPR deals with the fairness of pre-formulated declarations with reference to the UCT Directive in the application of informed data subject consent as a condition for lawful processing.

I. Pre-Formulated Declarations of Consent

The specification in Recital 42 GDPR that pre-formulated declarations of consent are to be provided "in an intelligible and easily accessible form, using clear and plain language,"[50] repeats the terminology used in Article 7(2) GDPR and Article 12(1) GDPR, and also seemingly echoes the formal fairness element in the UCT Directive. Article 5 UCT Directive states that, "[i]n the case of contracts where all or certain terms offered to the consumer are in writing, these terms must always be drafted in plain, intelligible language. Where there is doubt about the meaning of a term, the interpretation most favourable to the consumer shall prevail. .. ."[51] Given the clear overlap in terminology, it is pertinent to analyze the interpretation of these notions in the UCT Directive with reference to the Court of Justice case law.

Article 5 UCT Directive strongly relates to the principle of transparency with the Member States being explicitly required to include the transparency principle in their implementations with mere references to the Court's established practices regarded as insufficient.[52] Micklitz has noted in his analysis of the UCT Directive that transparency can be categorized as a sub-category of good faith via the principle of legitimate expectations which stems from the plainness and intelligibility standards.[53] The meaning of plain, intelligible language was analyzed by the Court of Justice in the Kasler judgement where the Court placed this requirement within

[47]GDPR, *supra* 5, at art. 7(2).

[48]The information requirements are further specified in, GDPR, *supra* 5, at art. 13 ("Information to be provided where personal data are collected from the data subject"); GDPR, supra 5, at art. 13 ("Information to be provided where personal data have not been obtained from the data subject"); *See* GDPR, *supra* 5, at sec. 5(2) (emphasis added).

[49]*See* GDPR, *supra* 5, at art. 12(1).

[50]GDPR, *supra* 5, at recital 42.

[51]Council Directive 93/13, of 5 April 1993 on Unfair Terms in Consumer Contracts, art. 5, 1993 O.J. (L 95) [hereinafter UCT Directive].

[52]Micklitz, *supra* note 43, at 142–45.

[53]*Id.* at 143.

المنارة للاستشارات
www.

the broader setting of providing information before consumers are bound by a contract.[54] It further stipulated that this requirement is not limited to grammatical intelligibility but must instead be understood broadly[55] in order to allow the consumer "to evaluate, on the basis of clear, intelligible criteria, the economic consequences for him which derive from it."[56] Plainness appears to relate to a term's legal effect including its consequences vis-à-vis ambiguous formulations and the requirement that such terms should not put the seller or supplier in an advantageous position.

In contrast, intelligibility incorporates a linguistic element in terms of legibility whereby, if the seller is aware or should have been aware—for example, if they had exercised reasonable care—that a term is linguistically unintelligible for a consumer, then the seller is required to ensure its intelligibility. This is particularly significant in relation to standard form contracts which must, according to this requirement, be designed plainly both optically and also in terms of editing.[57] In saying this, however, it should be noted that intelligibility inherently incorporates a qualitative aspect as well, in that the information provided must also accurately and adequately inform the consumer in order to facilitate informed consumer decision-making. More simply, making the terms legible should not result in a loss of nuance in relation to the nature of the contractual agreement regarding the rights and obligations contained therein. Consequently, the interpretation of the terminology in the UCT Directive that is common across the frameworks—plain and intelligible—appears to reflect the aims of the equivalent provisions in the GDPR. In saying this though, it is important to highlight the subtle differences in construction, but also the additional reference to the requirement that declarations of consent be drafted in an easily accessible form provided for in the GDPR. This requirement seems to further specify plainness and intelligibility as understood under the UCT Directive. In addition, one should also be aware of the insertion of the obligation for concise and transparent information and communications in Article 12 GDPR.

These differences raise three important observations. First, the addition of the terms concise and transparent in Article 12(1) GDPR appears to reflect both the inherent aims of the UCT Directive but also the important positioning of the transparency principle in the GDPR. This is also reflected in the further specification of the intelligibility requirement and thus the reference to the potential use of icons in the operation of the information requirements contained in Articles 13 and 14 GDPR.[58] Second, the use of the formal fairness element from the UCT Directive—both *ex ante* and *ex post* is indicative of the overarching role of the procedural fairness element in the GDPR. In particular, the use of this terminology and its application to both the information provision requirements[59] and any communication to the data subject,[60] show that the operation of the procedural fairness requirement extends beyond merely pre-formulated declarations of consent. This contrasts with the purely *ex ante* requirements in the UCT Directive. Finally, the specification in Article 12(1) GDPR that the information requirements must consider if the data subject is a child reflects the contextual nature of the procedural fairness element. Therefore, pre-formulated declarations depend on their intended use, and this is indicative of the fair balancing element in data protection fairness and hence, the requirement for data protection by design and by default in Article 25 GDPR.

In addition to the above comparisons, it is also important to note that Article 5 UCT Directive also provides for the *in dubio contra proferentem* rule whereby if a doubt exists in terms of meaning of a contractual term, the most favorable interpretation for the consumer must prevail. As noted by Rott however, there is a degree of uncertainty regarding the practical operation of this principle in that:

[54]Case C-26/13, Árpád Kásler, Hajnalka Káslerné Rábai v. OTP Jelzálogbank Zrt (Apr. 30, 2014), http://curia.europa.eu/.
[55]*Id.* at 71.
[56]*Id.* at 75.
[57]Micklitz, *supra* note 43, at 143.
[58]*See* GDPR, *supra* 5, at art. 12(7), Recital 60.
[59]*Id.* at arts. 13-14.
[60]*Id.* at arts. 15–22, 34.

المنارة للاستشارات
www.

> [I]f in case of an intransparent term one chose the consumer-friendly interpretation to start with, the term may not be held to be unfair. If, in contrast, the term was first tested for its fairness in its consumer-unfriendly interpretation, it might be unfair and therefore invalid; which would most likely benefit the consumer more than a consumer-friendly version of it.[61]

For our current purposes, it is important to note that it is unclear how this rule would play out in the data protection context given that personal data can be used for multiple purposes—for example, provided one of the conditions contained in Article 6(1) GDPR is satisfied, see Figure 3. More specifically, ambiguity in the terms relating to the use of personal data will largely be context-dependent but will also on the face of it be contrary to the requirements contained in the GDPR. The transparency principle is of key importance and controllers are required to provide accurate information. As noted by the Article 29 Working Party, controllers are required to provide full and specific information even if less information would be easier for the data subject to understand.[62]

Consequently, ambiguity in data protection would be seen as a violation of the transparency, fairness, and accountability principles. Controllers are required to take data subject rights and interests into account in the application of fair balancing and are also attributed the burden of proof in demonstrating their compliance with this requirement in line with procedural fairness—and more generally the burden of care in the application of fair balancing. For instance, as noted above in Section B(II), one can refer to Article 7(1) GDPR and the requirement to be able to demonstrate that the data subject has indeed consented. This is also indicative of the third component in the procedural fairness element, namely timeliness, as manifested in the requirement for controllers to reply without undue delay to data subjects' requests for information under Articles 15–22 GDPR. Therefore, the formal element of the UCT Directive must be viewed in tandem with fairness in the GDPR. In discussing Recital 42 GDPR, Svantesson observes that this provisions indicates that the GDPR should be understood as providing *lex specialis* guidance as to how unfairness in the UCT Directive should apply in the data protection setting.[63] Although there appears to be certainly merit to this observation at first glance, the substantive delineation in terms of protections as evidenced by recent enforcement actions may place such an observation in doubt. Instead, therefore, this reference may suggest that, rather than providing a confirmation of a *lex specialis* relationship, Recital 42 GDPR in fact indicates parallel, concurrent, but substantively distinct, fairness assessments, thus reflecting the differences vis-à-vis the Charter foundations of the respective frameworks as previously described. This contention will now be bolstered through an analysis of the substantive fairness element in the UCT Directive below.

II. Delineating Pre-Formulated and Individually Negotiated Terms

From the above, the formal fairness element in the UCT Directive appears to provide some interpretive guidance for the validity of pre-formulated declarations of consent. At the same time, it is to be placed alongside the operation of the data protection fairness principle and the GDPR as a secondary framework more generally.[64] That being said, however, aside from this reference to

[61]Peter Rott, *Unfair Contract Terms*, *in* Res. Handbook on EU Consumer and Cont. L. 287, 301 (Christian Twigg-Flesner ed., 2016), https://www.elgaronline.com/view/edcoll/9781782547365/9781782547365.00021.xml.

[62]Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent*, WP 187 (July 13, 2011); Article 29 Data Protection Working Party, *Opinion Guidelines on Consent under Regulation 2016/679*, WP 259 (Nov. 28, 2017);

[63]Dan Jerker B. Svantesson, *Enter the Quagmire—the Complicated Relationship between Data Protection Law and Consumer Protection Law*, 34 Computer L. & Security Rev. 7, 25 (2018), http://linkinghub.elsevier.com/retrieve/pii/S0267364917302558

[64]In a similar vein, see Michiel Rhoen, *Beyond Consent: Improving Data Protection through Consumer Protection Law*, 5 Internet Pol'y Rev. (2016), https://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-law.

المنارة للاستشارات
www.

the formal fairness element of the UCT Directive, Recital 42 GDPR also inserts a specific reference to the requirement that such pre-formulated declarations should not contain unfair terms. Hence, the recital seemingly refers to the substantive fairness element in the UCT Directive.

1. Giving Meaning to Unfair Terms

The substantive fairness element in the UCT Directive contains both good faith and significant imbalance components. According to Article 3(1) UCT Directive, a term will be regarded as unfair "if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer." There has been intense academic debate surrounding the meaning of good faith and significant imbalance. More specifically, as contracts are rarely contrary to the interests of traders, the potential openness of the test has been criticized.[65] In addition, good faith was somewhat alien to the common law tradition.[66] Although at first the UCT Directive had little real impact, in more recent years there has been a dramatic increase in the number of references from the national courts, thus facilitating the emergence of a deeper understanding of the Directive's substantive fairness element.[67]

More specifically, in endorsing the opinion of Advocate General Kokott in the Mohammed Aziz case, the Court of Justice found that in the determination of whether there is a significant imbalance the national court should take the national rules that would apply in the absence of a contractual agreement into consideration.[68] The Court further observed such an analysis would allow the national court to assess the extent to which the contract results in a less favorable legal situation and that such an assessment should include an examination of the legal situation of the consumer with regard to the means at their disposal under national law to prevent the continued use of unfair terms.[69] In the determination of the circumstances in which such an imbalance arises contrary to the good faith requirement, the Court of Justice stated that Recital 16 UCT Directive should be considered. In particular, in addition to indicating that good faith may be satisfied if the seller or supplier deals fairly and equitably with the consumer by taking their interests into account, Recital 16 UCT Directive further provides that the assessment of good faith necessitates the consideration of the bargaining power of both parties—including the specific consumer vulnerabilities[70]; whether the consumer was induced to accept the term; and also whether the goods or services were being sold or supplied by the special order of the consumer. As a consequence, the national court is required to assess whether the seller or supplier, dealing fairly and equitably with the consumer, could reasonably assume that the consumer would have agreed to such a term in individual contract negotiations taking the particular circumstances of the case into account.[71]

The Court of Justice has subsequently confirmed the judgement in Mohammed Aziz and found that a significant imbalance does not necessarily have to relate to an economic disparity but

[65]Rott, *supra* note 61, at 299.

[66]*See* Stephen Weatherill, EU Consumer Law and Policy 122 (Edward Elgar, 2005).

[67]Hans-W Micklitz & Norbert Reich, *The Court and Sleeping Beauty: The Revival of the Unfair Contract Terms Directive (UCTD)*, 51 Common Mkt. L. Rev. 771 (2014).

[68]Case C-415/11, Mohamed Aziz v. Caixa d'Estalvis de Catalunya, Tarragona i Manresa (Catalunyacaixa), (Mar. 14, 2013), http://curia.europa.eu/.

[69]*Id.* at 68.

[70]*See* Rott, *supra* note 61, at 301. The author notes that "[s]uch vulnerabilities can relate to inexperience but also to difficulties to get access to certain goods or services, due to poverty." For one example, the CJEU stated in Asbeek Brusse:

> [T]he consequences of the inequality existing between the parties are aggravated by the fact that, from an economic perspective, such a contract relates to an essential need of the consumer, namely to obtain lodging, and involves sums which most frequently, for the tenant, represent one of the most significant items in his budget. . . .

See Case C-488/11, Dirk Frederik Asbeek Brusse and Katarina de Man Garabito v. Jahani BV (May 30, 2013), http://curia.europa.eu/.

[71]Case C-415/11, *supra* note 68, at paras. 68, 76, 77.

المنارة للاستشارات
www.

instead can also be a consequence of a "sufficiently serious impairment of the legal situation in which that consumer, as a party to the contract, is placed, *vis-à-vis* a restriction of rights or a constraint on the exercise of such rights."[72] Importantly, in this context it is also necessary to examine Article 4(1) UCT Directive which stipulates that:

> [T]he unfairness of a contractual term shall be assessed, taking into account the nature of the goods or services for which the contract was concluded and by referring, at the time of conclusion of the contract, to all the circumstances attending the conclusion of the contract and to all the other terms of the contract or of another contract on which it is dependent.[73]

This provision highlights the importance of the individual circumstances of each case and, therefore, the significant role played by the national courts as the evaluators of the fairness of a specific term, given that the Court of Justice does not normally have access to the full facts of the case.[74] In this context, the role of the annexed grey-list, which provides an indicative list of unfair clauses, should also be acknowledged.[75] Indeed, although the Court of Justice has stated on several occasions that the adoption of this list is up to the Member States and that there is no presumption of unfairness unless otherwise provided by national law, according to the Invitel judgement the inclusion of a term in the list remains an essential element on which the national court can base its assessment.[76]

With this in mind, it is important to note that the UCT Directive is a product of its time in that in effect it amounts to a partial harmonization of consumer contract law, largely focused on information provision and transparency as adopted under Article 100a EEC (now Article 114TFEU). This Treaty provision forms the legal basis for the EU to adopt legislation for the approximation of laws for the functioning of the internal market. To clarify, Article 114 TFEU permits the EU legislator to regulate areas which are seen as obstacles to the proper functioning of the internal market. It should also be noted that, given the fact that the Directive is a minimum harmonization instrument,[77] Member States are not precluded from offering a higher level of protection. Establishing precise indicators for when a term is contrary to good faith is, therefore, a determination which remains challenging at the EU level. As a consequence, there is a large degree of disparity amongst the Member States with many opting to expand the protections—for example, if the existing protections were not already more expansive.[78] Accordingly, in order to truly assess the fairness of a particular term one is required to refer to the national courts.[79] The room for maneuver afforded by the minimum harmonization approach is illustrative of the tight reign that Member States have kept over national contract law, for more see Section D below. This is indicative of the Directive's restricted scope in that it only concerns terms that have not been individually negotiated.

From the above, therefore, one must question how the substantive fairness element in the UCT Directive overlaps with the principle of fairness in data protection in order to interpret unfair terms in the context of pre-formulated declarations of consent. The need for such an assessment

[72]Case C-226/12, Constructora Principado SA v. José Ignacio Menéndez Álvárez (Jan. 16, 2014), http://curia.europa.eu/.

[73]UCT Directive, *supra* 51, at art. 4(1).

[74]Rott, *supra* note 61, at 300.

[75]*See* UCT Directive, *supra* 51, at art. 4(1).

[76]Case C-472/10, Nemzeti Fogyasztóvédelmi Hatóság v. Invitel Távközlési Zrt, (Apr. 26, 2012), http://curia.europa.eu/.

[77]According to Article 8 UCT Directive, the Directive it is a minimum harmonization instrument. UCT Directive, *supra* 51, at art. 8.

[78]For a discussion of the various implementations, see HANS SCHULTE-NÖLKE ET AL., EC CONSUMER LAW COMPENDIUM: THE CONSUMER ACQUIS AND ITS TRANSPOSITION IN THE MEMBER STATE [I.E. STATES] 197-261 (Sellier European Law Publishers, 2008).

[79]*See* Case C-237/02, Freiburger Kommunalbauten GmbH Baugesellschaft & Co. KG v. Ludger Hofstetter and Ulrike Hofstetter, 2004 E.C.R. I-03403 (ruling that it is for the national courts to decide on unfairness under Article 3 UCT Directive).

المنارة للاستشارات
www.

is particularly clear given that the UCT Directive focuses on economic considerations in comparison to the fundamental rights focus of the GDPR. In this vein, one can refer to the recent EDPS opinion on the proposed Directive on certain aspects concerning contracts for the supply of digital content[80] in which the EDPS criticizes the use of Article 114 TFEU as a legislative basis concerning matters involving personal data due to the availability of Article 16 TFEU. Arguably this points to a larger issue with relying on frameworks based on Article 114 TFEU, and, thus, their suitability to cater for social rights orientated concerns rather than the market integration centered mandate understood more readily to be the focus point of Article 114 TFEU. To clarify, this is not to suggest that Article 114 TFEU cannot be used to harmonize protections but rather to question how this might affect the protection goal.

Although the relationship between Article 114 TFEU and Article 16 TFEU is a matter requiring more detailed analysis, for our current purposes it is sufficient to conclude that the precise effect of such considerations remains to be seen. But, given the potential distinction, it is necessary to question the overlap between the reference to the prohibition of unfair terms and the last sentence in Article 7(2) GDPR which, as noted above, states that, "[a]ny part of such a declaration which constitutes an infringement of this Regulation shall not be binding."[81] Therefore, although it is clear that any part of a declaration, pre-formulated or not, which infringes the GDPR will not be binding, it is uncertain how this clarification differs substantively from the UCT Directive fairness assessment of pre-formulated declarations. As mentioned in the previous sub-Section, Svantesson suggests that the reference to the assessment of unfair terms under the UCT Directive could be viewed as providing *lex specialis* specification of the rules therein through the requirements in the GDPR.[82] Due to the fundamental deviations underlying the frameworks however, one should question such a conclusion. In support of this, one can refer to the common position taken by various national consumer protection agencies through the Consumer Protection Collaboration Network regarding the terms of service of social networking sites which clearly focused on more traditional cross-border consumer contract issues. These issues include clauses relating to jurisdiction, the identification of commercial communications, the waiving of liability, the removal of content and unilateral rights to change, determine the scope of and terminate agreements.[83] Accordingly, instead of incorporating an assessment of the fairness of terms in line with data protection—which would relate more to the application of the transparency principle and the validity of the data subjects' consent—the common position focuses on issues more aligned with traditional B2 C cross-border contract issues. Such a distinction allows for the differentiation in the respective frameworks' intent and their underlying policy objectives. This also appears to be reflected in the judgements of—at least some—national courts where national law contract formation requirements are satisfied.

Helberger, Borgesius, and Reyna highlight in particular the cases taken by the Federation of German Consumer Organizations (*Verbraucherzentrale Bundesverband*) against Facebook which have confirmed that the UCT Directive applies to situations concerning personal data processing.[84] Indeed, building on the authors' overview one can also refer to a recent judgement of the Berlin Regional Court which found eight clauses in Facebook's terms of use to be invalid

[80] *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) 0634 final (Dec. 9, 2015).

[81] GDPR, *supra* 5, at art. 7(2).

[82] Svantesson, *supra* note 63.

[83] *Common Position of National Authorities within the CPC Network Concerning the Protection of Consumers on Social Networks*, European Commission (Mar. 17, 2017), http://europa.eu/rapid/press-release_IP-17-631_en.htm.

[84] Natali Helberger et al., *The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law*, 54 Common Mkt. L. Rev. 1427, 1452 (2017).

المنارة للاستشارات
www.

under the German implementation of the UCT Directive.[85] For example, the Berlin Court found that terms specifying that pre-formulated declarations of consent permitting Facebook to use the individual's name and profile picture for commercial, sponsored, or related content and to transfer personal data to the US were unfair. The court, however, also rejected several submissions against Facebook's privacy policy by finding that the policy only contains information about procedures and thus no contractual provisions.[86] This judgement, therefore, appears to demonstrate the divergence between the respective realms of data and consumer protection.

To illustrate this difference more tangibly, it is significant to refer to the fallout from the Facebook-WhatsApp merger and the change in privacy policy that WhatsApp imposed on its users in August 2016, as well as the subsequent regulatory responses. As background, while Mark Zuckerberg—Facebook's CEO—made public assurances that no changes would take place in the way WhatsApp uses personal data from users at the time of the notification of the Facebook-WhatsApp acquisition,[87] within two years after the approval of the merger by the European Commission, Facebook introduced an update of WhatsApp's privacy policy that would enable the company to start using data from WhatsApp to better target ads on Facebook and Instagram.[88] As summarized by Zingales,[89] this attracted the attention of several data protection authorities and resulted in a coordinated action by the Article 29 Working Party. The coordinated action aimed to clarify the concerns associated with the merger and resulting change in privacy policy and has resulted in an ongoing correspondence between the Working Party and the company.[90] More specifically, the Working Party's letter sent on October 24, 2017, specifies WhatsApp's failure to satisfy each of the conditions for consent and in particular their failure to adequately inform, specify the intended purposes, and more generally comply with the transparency principle and the freely given stipulation in the definition of consent.[91]

In addition to arousing the interest of data protection authorities, however, the developments since the Facebook-WhatsApp merger have also caught the eye of consumer protection authorities. More specifically, the Federation of German Consumer Organizations sought an injunction to stop the continued data-sharing and the deletion of the data already transferred to Facebook.[92]

[85]Landgericht Berlin [LG Berlin] [Berlin Regional Court] Jan. 1, 2018, 16 O 341/15; For a case description, see *Facebook Verstößt Gegen Deutsches Datenschutzrecht*, Verbraucherzentrale Bunderesvesband (Feb. 12, 2018), https://www.vzbv.de/pressemitteilung/facebook-verstoesst-gegen-deutsches-datenschutzrecht.

[86]*Id.*

[87]Jessica Guynn, *Privacy Groups Urge FTC to Probe Facebook's Deal to Buy WhatsApp*, Los Angeles Times (March 6, 2014), http://www.latimes.com/business/technology/la-fi-tn-privacy-groups-urge-ftc-to-probe-facebooks-whatsapp-deal-20140306-story.html.

[88]*Looking Ahead for WhatsApp*, WhatsApp, https://blog.whatsapp.com/10000627/Looking-ahead-for-WhatsApp?l%3den.

[89]Nicolo Zingales, *Between a Rock and Two Hard Places: WhatsApp at the Crossroad of Competition, Data Protection and Consumer Law*, 33 Computer L. & Security Rev. 553 (2017).

[90]*See Article 29 Data Protection Working Party, Letter to WhatsApp*, Article 29 Data Protection Working Party (October 27, 2016), https://www.cnil.fr/sites/default/files/atoms/files/20161027_letter_of_the_chair_of_the_art_29_ wp_whatsapp.pdf; *Article 29 Data Protection Working Party, Letter to WhatsApp*, Article 29 Data Protection Working Party (December 16, 2016), ec.europa.eu/newsroom/document.cfm?doc_id%3d40927; *Article 29 Data Protection Working Party, Letter to WhatsApp*, Article 29 Data Protection Working Party (October 24, 2017), https://ec.europa.eu/newsroom/just/document.cfm?doc_id%3d47964.

[91]More specifically, the letter states that WhatsApp failed to: (1) Inform the data subject and thus provide adequate information on the sources and categories of data and a list of recipients within the Facebook family of companies, that the consent obtained; (2) satisfy the freely given requirement due to the "the pre-eminence of WhatsApp's messaging service . . . and the extent to which Facebook's social networking service is embedded into the digital lives of European citizens," and the adoption of a take it or leave it approach; (3) sufficiently specify the intended purposes in that the options offered by WhatsApp were insufficiently granular; and (4) comply with the transparency principle given the use of pre-ticked boxes for the purpose of "improving Facebook ads and products experiences" which failed to satisfy the unambiguous criterion and as a consequence the overarching requirement for fair processing due to the lack of transparency and sufficient data subject controls. *Article 29 Data Protection Working Party, Letter to WhatsApp*, Article 29 Data Protection Working Party (October 24, 2017), https://ec.europa.eu/newsroom/just/document.cfm?doc_id%3d47964.

[92]*See* Helberger, *supra* note 84, at 142.

المنارة للاستشارات
www.

Furthermore, on May 11th, 2017, the Italian Competition and Consumer Protection Authority (*Autorita' Garante della Concorrenza e del Mercato* (AGCM)) adopted two decisions in its proceedings against WhatsApp.[93] Nevertheless, in line with the common position taken by a number of national consumer protection agencies, the AGCM rulings appear to diverge from the approach taken by the Article 29 Working Party in relation to the information requirements and, thus, the expectations of the respective enforcement agencies—thereby indicating deviations in substantive requirements. The action taken by the Article 29 Working Party focused on the failure to inform the data subjects of the sources and categories of data and to sufficiently specify the intended purposes. The Article 29 Working Party viewed these failures to be in violation of the transparency principle in the GDPR. In contrast, similar to the common position adopted by national consumer protection agencies, the AGCM, in its proceedings concerning the UCT Directive, focused instead on the fairness of clauses regarding issues such as inter alia the choice of jurisdiction and law clauses, the unilateral authority to interrupt the service without reason or advance notice, and to rescind or terminate the contract.[94]

From the diverging interpretations by the relevant enforcement authorities, the formulation of Recital 42 GDPR, and the specific reference to the limitation in scope to pre-formulated declarations, it can be concluded that the Recital aims to clarify that pre-formulated privacy policies may be "unfair" under the distinct yet complementary UCT Directive protections. It is suggested, therefore, that the UCT Directive and the GDPR operate in an independent but complementary manner. This appears to be indicative of the bolstered protections for data subject consent, the common reliance on pre-formulated terms—especially in the ISS context—and hence, the apparent need to protect data subject-consumers from consenting to terms that they would otherwise not have agreed to had they been individually negotiated.

2. Pre-Formulated Versus Individually Negotiated and the Importance of Price

From the above, it is important to reiterate that the UCT Directive is a minimum harmonization instrument and is hence reliant on national law implementations, which can offer a higher degree of protection. This approach has consequently led to a large degree of disparity across the Member States, which is a reflection of diversity in terms of legal traditions and approaches in national contract law. Furthermore, this also reflects the focus of the UCT Directive on terms not individually negotiated. Indeed, as per Article 3(2) UCT Directive, terms drafted in advance are always considered as not being individually negotiated and where there is doubt the burden of proof rests with the seller or provider. As previously mentioned, this focus on pre-formulated terms reflects the underlying assumption that consumers who actually engage in negotiations with traders are protected from risk. Weatherill observes, however:

> [T]his is by no means uncontroversial. One might go so far as to adopt precisely the opposite perspective and argue that face-to-face discussion deepens the risk that the economically powerful trader will exploit the consumer. However, the Directive's limitation to terms that have not been individually negotiated demonstrates a suspicion of "mass-produced" contracts, at least at the threshold of jurisdiction to check enforceability.[95]

The delineation of the UCT Directive's scope is important, given that it reflects the ongoing importance of national law and courts, which are of substantial significance in the shaping the application of the protections.

[93]One of these established the unfairness of particular terms under the Italian implementation of the UCT Directive, whereas the other qualified the process through which WhatsApp obtained the consent of the user as unfair and aggressive under the Italian implementation of Articles 5, 8 and 9 of the UCP Directive.

[94]*See WhatsApp Fined for 3 Million Euro for Having Forced Its Users to Share Their Personal Data with Facebook*, Antitrust Authority, https://en.agcm.it/en/media/press-releases/2017/5/alias-2380

[95]Weatherill, *supra* note 66, at 118.

المنارة للاستشارات
www.

Although it is hard to imagine an individually negotiated B2 C term especially in the ISS context, this does raise interesting questions in terms of practical application. Would the negotiation of any part of a contract render it pre-formulated or individually negotiated? And further, how are terms classified as pre-formulated in practice? In this regard, one can refer to Article 3(2) UCT Directive which stipulates that:

> [A] term shall always be regarded as not individually negotiated where it has been drafted in advance and the consumer has therefore not been able to influence the substance of the term, particularly in the context of a pre-formulated standard contract.
>
> The fact that certain aspects of a term or one specific term have been individually negotiated shall not exclude the application of this Article to the rest of a contract if an overall assessment of the contract indicates that it is nevertheless a pre-formulated standard contract.
>
> Where any seller or supplier claims that a standard term has been individually negotiated, the burden of proof in this respect shall be incumbent on him.[96]

In commenting on this provision and hence, the notion of individual terms, Micklitz argues that the term pre-formulated does not have to be interpreted strictly.[97] Micklitz substantiates this observation with reference to two important points. First, contracts between private persons based on individual negotiations are not included within the scope of the UCT Directive, and second, the core terms relating to the "price/quality ratio and the main subject matter of the contract" are not subject to review.[98]

The first of these points inherently points towards the personal scope of the Directive and, thus, the specification in Article 1(1) UCT Directive that the Directive targets contracts concluded between a seller or supplier and a consumer. Regarding the second of these points, it is important to highlight Article 4(2) UCT Directive. This provision states that an:

> [A]ssessment of the unfair nature of the terms shall relate neither to the definition of the main subject matter of the contract nor to the adequacy of the price and remuneration, on the one hand, as against the services or goods supplies [*sic*] in exchange, on the other, in so far as these terms are in plain intelligible language.[99]

Consequently, the exemption of these core terms restricts the application of the substantive fairness element to the more peripheral contractual aspects—provided such terms are stipulated in plain intelligible language and in line with the formal fairness element—hence seemingly minimizing the impact on freedom of contract.[100] The key point which emerges from Article 4(2) UCT Directive, therefore, is that the Directive does not wish to control the fairness of the "price."[101] In the context of pre-formulated declarations of consent, the question thus becomes: What constitutes a price? This is a matter for the national courts to determine with reference to the specific facts of the case. It is a hotly contested topic, given that distinguishing the specific limits of this notion remains challenging. More specifically, the case law on this issue has highlighted the

[96]UCT Directive, *supra* 51, at art. 3(2).
[97]Micklitz, *supra* note 43, 135–36.
[98]*Id.*
[99]UCT Directive, supra 51, at art. 4(2).
[100]Donnelly, *supra* note 44, at 248.
[101]Rott, *supra* note 61, at 294.

المنارة للاستشارات
www.

stickiness of this concern,[102] and this has resulted in some disparity in interpretation between the national courts and the Court of Justice.[103]

It should be noted, however, that even if a term under assessment is deemed to fall within the exemption provided in Article 4(2) UCT Directive, it is still subject to an overarching transparency requirement given that this same provision mandates that such terms be presented in plain intelligible language.[104] Given the focus of the present Article, however, it is necessary to explore this issue further. Hence, the question becomes one of how the exclusion of the "adequacy of the price and remuneration, on the one hand, as against the services or goods supplies [sic] in exchange, on the other,"[105] may affect the application of the UCT Directive in the context of pre-formulated declarations of consent. This raises an important fundamental sub-question: Are personal data to be considered a "price"? Such a finding would exempt the provision of personal data from the substantive fairness test, which would appear odd given the aim of pre-formulated declarations of consent. Although the ability to offer higher levels of protection remains and, thus, extends to the possibility of excluding the exemption provided in Article 4(2) UCT Directive in the national implementation,[106] the lack of a harmonized approach runs contrary to aims of the GDPR if personal data are positioned as the price.

Building on this discussion, one can refer again to the above delineation in the substantive application of the assessment of unfair terms in the UCT Directive and the fairness principle in the GDPR. Given that certain consumer protection authorities appear to position personal data as a *de facto* price and thus a core term, the substantive fairness element in the UCT Directive—at least unless otherwise provided for in the national implementation—does not apply in the enforcement of the Directive's protections.[107] Importantly, this does not affect the application of the GDPR's fairness principle. Although it will be discussed in more detail below, it is worth noting that this nuanced point perhaps adds further clarification in terms of delineating the substantive application of the fairness protections in the UCT Directive and the GDPR. Nevertheless, it is important to re-emphasize that this will depend on the national implementations and thus on whether national transpositions of the UCT Directive, or indeed the prior existing law, extend the substantive protections to core terms. As noted by Helberger, Borgesius, and Reyna, therefore, consumer law could be positioned as an important instrument in the assessment of the fairness of the conditions under which consumers agree to personal data processing.[108] Nevertheless, due to the minimum harmonization approach in the UCT Directive and the more specifically tailored rules in the GDPR, there is potential for disparity. It is thus argued that a violation of consumer law would merely result in the addition of supplementary enforcement mechanisms, rather than a further tailoring of the data protection requirements, as any breach of the GDPR will not be binding in line with Article 7(2) GDPR. Nonetheless, this is certainly not a straightforward matter.

As described above in Section B(I), the right to data protection aims to protect individual control over personal data. In its construction, this fundamental right recognizes the benefits

[102]*See id.* at 293 (providing an example of financial services).

[103]*See* Case C-92/11, RWE Vertrieb AG v. Verbraucherzentrale Nordrhein-Westfalen eV (Mar. 21, 2013), http://curia.europa.eu/; *Contra* Office of Fair Trading v. Abbey National plc & Others [2009] UKSC 6 [2009] 3 WLR 1215; *see also* Rott, *supra* note 61, at 294.

[104]Indeed, in the *Kásler* case the Court of Justice found that it was for the national court to decide whether "the average consumer, who is reasonably well informed and circumspect" would have been aware of the information specifically relevant for the circumstances of the case thus recognizing the importance of the cognitive capacity of the average consumer for the first time. *See* Case C-26/13, *supra* note 54.

[105]UCT Directive, *supra* 51, at art. 4(2)

[106]Case C-484/08, Caja de Ahorros y Monte de Piedad de Madrid v. Asociación de Usuarios de Servicios Bancarios (Ausbanc), 2010 E.C.R. I-04785.

[107]In support of this point, one can refer to common position of the national consumer authorities, but also more explicitly to the recent rulings by the Italian consumer authority on the fairness of the WhatsApp privacy policy changes.

[108]Helberger, *supra* note 84, at 1451.

المنارة للاستشارات
www.

of personal data processing but also aims to mitigate this by targeting the prevention of disproportionate impacts on individuals.[109] This is reflected in the triangular structure of Article 8 of the Charter—for example, controller obligations, data subject rights and the monitoring activities of the authorities.[110] Data subject control, however, remains key in the operation of the GDPR, given that the framework aims to not only protect fundamental rights and freedoms in general, but also the right to data protection in particular where personal data are processed in Article 1(2) GDPR. That being said, personal data are seen by many as the currency through which ISS are provided with certain consumer protection authorities clearly positioning personal data as a price.[111] Furthermore, the UCT Directive inherently assumes that some form of price will be exchanged in the operation of its provisions as evidenced by the exclusion of the core terms from the substantive fairness element assessment at the EU level. Therefore, the determination of what will be classified as a price is of clear importance. The following Section aims to more specifically tackle the categorization of personal data as a price, given that it is a particularly thorny issue in the alignment of the protections offered by the UCT Directive and the GDPR, and as it has been at the root of the reforms of the consumer law framework.

D. The Economic Value of Personal Data and Fair Personal Data Processing

The need for some form of value exchange or price is indicative of the fact that in order to assess the validity of the contract formation, one is required to refer to the national level. This reflects the failed attempts to harmonize contract formation at the EU level. More specifically, the jettisoning of large parts of the Consumer Rights Directive[112] during the negotiations[113] and the failed Regulation of the European Parliament and of the Council on a Common European Sales Law —known as the Optional Instrument—are evidence of how controversial the harmonization of contract formation has been in practice. This is of particular relevance for the current analysis as the European Commission proposed the Digital Content Directive[114] as a means of filling the gap left by the failure of the Optional Instrument via a dilution of the Regulation's ambitions—thus leaving the laws governing contract formation in the hands of Member States—instead aiming to recognize that data, including personal data, can be positioned as a form of payment. In support of this contention one can refer, for instance, to Article 5(b) of the failed Optional Instrument which aimed to recognize the validity of "contracts for the supply of digital content whether or not supplied on a tangible medium which can be stored, processed or accessed, and

[109]As noted by Ferretti, data protection regulates "an accepted exercise of power." *See* Federico Ferretti, *Data Protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights?*, 51 COMMON MKT. L. REV. 843, 849 (2014).

[110]*See* Gloria González Fuster, *Beyond the GDPR, above the GDPR*, INTERNET POL'Y REV. (November 30, 2015), http://policyreview.info/articles/news/beyond-gdpr-above-gdpr/385.

[111]For instance, in the AGCM's analysis of the WhatsApp change in policy and the validity of consent, the authority refused to accept WhatsApp's claim—with reference to the EDPS opinion—that personal data could not be construed as counter-performance. The AGCM found, with reference to the recent common position on the application of consumer protection in the context of social media, that consumer protection and competition law and indeed, the company itself all recognize the economic value of the data. *See* Zingales, *supra* 89.

[112]Directive 2011/83, 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 Text with EEA relevance, 2011 O.J. (L 304) 64.

[113]IRIS BENOHR, EU CONSUMER LAW AND HUMAN RIGHTS 31-33 (OUP Oxford, 2013).

[114]*Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, at art. 11, COM (2015) 0634 final (Dec. 9, 2015) [hereinafter Digital Content Directive (Commission proposal)].*

المنارة للاستشارات
www.

re-used by the user, irrespective of whether the digital content is supplied in exchange for the payment of a price."[115]

In simple terms, this failed proposal aimed to recognized that there was no need for a price in order for a contract to be formed. In essence, by proposing the Digital Content Directive the Commission wished to avoid the problems of the past associated with harmonizing contract formation at the EU level, and instead aimed to extend protections to consumers in situations where personal data are effectively used as the means of payment. Such changes are also manifested in the "new deal for consumers" announced by the Commission and hence, the updating of the consumer *acquis*.[116] There is now a Compromise version of the Directive and, according to Article 1 Digital Content Directive (Compromise), the instrument aims to 'lay down common rules on certain requirements concerning contracts between traders and consumers for the supply of digital content or a digital service'.[117] More specifically, this provision goes on to note that the Directive aims in particular to establish rules on '(1) conformity of digital content/service with the contract; (2) remedies in case of the lack of such conformity or a failure to supply and the modalities for the exercise of those remedies and; (3) modification and termination of such contracts.'[118]As such, the Directive will extend the protections provided to consumers by affording concrete consumer rights and remedies. This is significant as currently at the EU level an infringement of the data protection framework may mean little in terms of consequences for a service contract.[119] But, despite these good intentions, the Directive raises a number of difficulties from a data protection and privacy perspective. It is important to consider these in detail and in particular, the extension of consumer law to so-called 'free' services, as the determination of what will be considered as a price or core term under the scope of the UCT Directive is of key importance in assessing how this Directive may interact with the GDPR. Hence, this Section will first analyze the Digital Content Directive (Compromise) with specific reference to the role of personal data in the various draft versions of the legislation in order to better understand the final Compromise. Building on this, the analysis will then turn to an examination of how the UCT Directive could be interpreted in the context of pre-formulated declarations of data subject consent.

I. Core terms, Passive and Active Collection and Data as Counter-Performance

Article 3(1) of the Commission draft of the Digital Content Directive provided that the proposal "shall apply to any contract 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*."[120] Hence, the Commission draft explicitly recognized: (1) the active as opposed to passive supply of data—including personal data—as (2) counter-performance. Both of these points were

[115]*Proposal for a Regulation of the European Parliament and of the Council on a Common European Sales Law*, COM (2011) 0635 final (Oct. 11, 2011).

[116]*A New Deal for Consumers: Commission Strengthens EU Consumer Rights and Enforcement*, EUR. COMMISSION (Apr. 11, 2018), http://europa.eu/rapid/press-release_IP-18-3041_en.htm.

[117]Compromise version, Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content and digital services, Compromise version PE -CONS 26/19 (April 3, 2019) [hereinafter Digital Content Directive (Compromise)].

[118]*Id.*

[119]*See* Helberger, *supra* note 84, at 1440. Indeed, as noted by Helberger:

> [A clear] benefit of extending the scope of consumer law to data-related issues lies in giving consumers concrete rights against sellers if information obligations are violated. If a data controller breaches data protection law's information obligations, the processing may become unlawful. That unlawfulness, however, says little about the consequences for a possible contractual relationship between seller and consumer.

[120]Digital Content Directive (Commission proposal), *supra* 114, at art. 3(1) (emphasis added).

المنارة للاستشارات
www.

heavily criticized, in particular by the EDPS's opinion on the proposal.[121] The final compromise deletes all explicit references to the active or passive provision of personal data and the term counter-performance. However, the Directive more fundamentally retains the references to the fact that the provision of personal data gives rise to the application of the protections in the Directive. More specifically, Article 3(1) Digital Content Directive (Compromise) provides that:

> This Directive shall apply to any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price.
>
> This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer and *the consumer provides or undertakes to provide personal data to the trader, except where the personal data* provided by the consumer *is exclusively processed by the trader for supplying the digital content or digital service* in accordance with this Directive *or* for the trader *to comply with legal requirements* to which the trader is subject, *and the trader does not process this data for any other purpose*.[122]

There are some subtle and arguably significant differences between the compromise version and the draft Article 3(1) in the Commission proposal outlined above. However, the Compromise version of the Directive still raises several difficulties from a data protection and privacy perspective which can be largely placed within two categories general reflecting the points made above in relation to the Commission draft proposal namely: (1) The positioning of personal data as a *de facto* 'price' in a consumer contract and; (2) the delineation of the types of personal data within the Digital Content Directive's scope of protection. The purpose of this Section therefore, is to analyze these issues in light of the Commission, European Parliament and Council versions and the final Compromise, as both elements present key challenges from a data protection and privacy perspective.

1. Passive and Active Collection and the ePrivacy Directive

As highlighted above, in their draft Digital Content Directive, the Commission confusingly drew a distinction between passive and active personal data collection in Article 3(1) of the proposal. This distinction was further specified in Recital 14 of the Commission draft. From these provisions, it is clear that the intention of the proposal was to exclude personal data such as IP addresses and "other automatically generated information such as information collected and transmitted by cookies, without the consumer actively supplying it, even if the consumer accepts the cookie"[123] from the scope of application. To add to the confusion, the Commission draft Recital 14 went on to note that the proposed Directive "should also not apply to situations where the consumer is exposed to advertisements exclusively in order to gain access to digital content."[124] Although the Parliament amendments proposed the deletion of this distinction,[125] the Council version retained the separation.[126] As such, both the Commission proposal and the proposed Council modifications envisaged a distinction between the active and passive provision of data and

[121] *See Opinion on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content*, EUR. DATA PROTECTION SUPERVISOR, https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en_0.pdf.

[122] Digital Content Directive (Compromise), *supra* 117, at art. 3(1) (emphasis added).

[123] Digital Content Directive (Commission proposal), *supra* 114, at recital 14.

[124] *Id.*

[125] *Report on the proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content*, at recital 14 (Nov. 27, 2017), http://www.europarl.europa.eu/doceo/document/A-8-2017-0375_EN.html. [hereinafter Digital Content Directive (Parliament draft)]

[126] More specifically, in footnote 15 of its general approach which adds nuance to its modified version of Article 3(1), the Council indicates its intention to add a specification in the Recitals to the effect that:

المنارة للاستشارات
www.

significantly this has found its way into the Compromise Directive. In this regard it is interesting to refer to Recital 14 Digital Content Directive (Compromise). This provision states *inter alia* that the Directive should:

> [N]ot apply to situations where the trader only collects metadata such as information concerning the consumer's device or the browsing history, except where this situation is considered a contract under national law. It should also not apply to situations where the consumer, without having concluded a contract with the trader, is exposed to advertisements exclusively in order to gain access to digital content or a digital service. However, Member States should remain free to extend the application of the rules of this Directive to such situations or to otherwise regulate such situations which are excluded from the scope of this Directive.[127]

This Recital therefore, appears to maintain the distinction that was in the Commission and Council versions and this raises two concerns. First, it appears to assume that advertising is separate from any contract formation – albeit while this remains an issue in the competence of the Members States; and second, it draws an odd distinction between different types of personal data. Hence, browsing on sites that do not require log-in information is deemed distinct from visiting a social networking site with only the latter invoking the operation of the compromise Directive. Nevertheless, such an interpretation seemingly disregards the fact that both IP addresses and cookies are widely considered as personal data and that personal data processing for online behavioral advertising purposes requires the consent of the data subject—for example, as confirmed by the Article 29 Working Party in several opinions.[128]

More specifically, although as specified above in Figure 3, contract[129] and legitimate interest[130] may be deemed appropriate in a B2 C ISS context under the scope of the GDPR, their applicability to the collection of such passive data provision in the current context is unlikely for two specific reasons. First, within the meaning of the draft versions of the proposal[131] and Article 3(1) Digital Content Directive Compromise, the provision of personal data necessary for the performance of a contract is excluded from the Directive's scope of application. Second, in relation to IP addresses, although one cannot deny the potential application of other conditions for lawful processing—such as legitimate interest in Article 6(1)(f) GDPR, as confirmed in the Breyer case—,[132] in the context of online behavioral advertising, consent is often the condition most likely to be deemed

---

> [T]his Directive should not apply to situations where the supplier only collects metadata, the IP address or other automatically generated information such as information collected and transmitted by cookies, except where this is considered as a contract by national law. Similarly, this Directive should also not apply to situations where the consumer, without having concluded a contract with the supplier, is exposed to advertisements exclusively in order to gain access to the digital content or digital service. Member States, however, should remain free to extend the application of the rules of this Directive to such situations or to otherwise regulate such situations which are excluded from the scope of this Directive.

Contracts for the supply of digital content and digital services, 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)—General approach, at art. 3(1) (June 1, 2017), http://data.consilium.europa.eu/doc/document/ST-9901-2017-ADD-1/en/pdf [hereinafter Digital Content Directive (Council draft)].

[127] Digital Content Directive (Compromise), *supra* 117, at recital 14.

[128] *See Opinion on Online Behavioural Advertising*, *supra* note 34.

[129] GDPR, *supra* 5, at art. 6(1)(b).

[130] *Id.* at art. 6(1)(f).

[131] As per Article 3(4) of the Commission and Parliament drafts and Article 3(1) of the Council version.

[132] The specific exclusion of IP addresses is also interesting given the recent CJEU judgement which found dynamic IP addresses to be personal data. *See* Case C-582/14, Breyer, Patrick Breyer v. Bundesrepublik Deutschland (Oct. 19, 2016), http://curia.europa.eu/; Frederik Zuiderveen Borgesius, *The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition*, 3 EUR. DATA PROTECTION L. REV. 130 (2017).

المنارة للاستشارات
www.

applicable, as the fair balancing act required under Article 6(1)(f) GDPR is unlikely to be satisfied. Of course, this does not comprehensively exclude the potential for advertising that does not require the consent of the data subject—contextual advertising or personal data processing that relies upon the legitimate interest or contract conditions which may relate for example to security purposes or processing necessary for the provision of a service—from being excluded from the scope of the Directive.

Indeed, this point appears to be reflected in the Parliament's proposed modifications to the Digital Content Directive, given that rather than referring to processing that is strictly necessary for the performance of a contract requested by the consumer—for example, as in the Commission version—reference was made to personal data "exclusively processed by the trader for supplying, maintaining the conformity of or improving this digital content or service."[133] Therefore, to summarize the above: The point proposed here is that this draws a line between different types of personal data in a context where the processing of both types requires the consent of the data subject under data protection and privacy law provisions.[134] Although by removing the terms passive and active, the Compromise Directive aims to avoid the problems associated with delineating based on the manner in which the personal data is provided, the difficulties from a data protection and privacy perspective remain. This criticism is even clearer in the context of cookies.

Building on the above, the disregard for the *lex specialis* protections provided for in Article 5(3) of the e-Privacy Directive is striking.[135] In short, Article 5(3) ePrivacy Directive[136] essentially provides for a higher degree of protection for the use of cookies or cookie-like technologies when used for non-functional purposes, by essentially mandating user consent as defined in the GDPR. Cookies come within the functional cookies exemption if either: (a) They are used "for the sole purpose of carrying out the transmission of a communication over an electronic communications network";[137] or (b) the cookie is "strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."[138] In its opinion on the exemptions, the Article 29 Working Party has noted that these are to be interpreted narrowly, and that, therefore, cookies for user tracking, third party advertising, or first party analytics, inter alia, do not come within their scope.[139] Article 5(3) ePrivacy Directive, therefore,

[133]Digital Content Directive (Parliament draft), *supra 125*, at Article 3(4).

[134]To clarify, the data protection and privacy framework does separate certain categories as being worthy of added protection—for instance, sensitive personal data under Article 9 GDPR and traffic and location data under the ePrivacy Directive. But, unlike the proposed Digital Content Directive, the purpose here is to identify categories of data that merit further protection, rather than drawing distinctions between data sets which both fall under the personal data definition thereby seemingly weakening protection. In this regard, it is also important to draw a distinction with the right to data portability and the discussion regarding whether this new right applies to both provided and processed data. In short, the difference here is that the proposed Digital Content Directive aims to create a distinction between personal data sets that are both provided by the data subject under the data protection and privacy framework, whereas the discussion regarding the scope of the right to data portability relates to the separation between provided personal data and processed data which may incorporate IP protection or other investments by data controllers. For a description of this processed/provided discussion, see Gianclaudio Malgieri, "'*User-Provided Personal Content' in the EU: Digital Currency between Data Protection and Intellectual Property*," Int'l Rev. of L. Computers & Tech. 1, 12–14 (2018).

[135]Directive 2002/58, of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on privacy and electronic communications), 2002 O.J. (L 201) 1, 37–47 [hereinafter ePrivacy Directive].

[136]*See* Directive 2009/136/EC Directive 2009/136/EC, of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection, 2009 O.J. (L 337) 11.

[137]ePrivacy Directive, *supra 135*, at art. 5(3).

[138]*Id.*

[139]Article 29 Working Party, *Opinion 04/2012 on Cookie Consent Exemption*, WP 194 (June 7, 2011) 1, 9–11, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2012/ wp194_en.pdf.

المنارة للاستشارات
www.

essentially denies the availability of the other conditions available in Article 6(1) GDPR for the processing of such personal data.[140] The distinction is justified as such methods are deemed to interfere with the terminal equipment—construed to mean consumer electronic devices and not just mobile phones—and, thus, the private sphere of the individuals concerned. This point is exemplified in the wording of Article 5(3) ePrivacy Directive which refers to the accessing of information stored or the storing of information, rather than the narrower category of personal data which refers to information which must relate to an identified or identifiable natural person as per Article 4(11) GDPR. It is therefore hard to understand how this differentiation between types of personal data aligns with the requirement of consent for the storing or accessing of information already stored on the terminal equipment of users—like cookies—as provided for in Article 5(3) ePrivacy Directive.[141]

Malgieri, in his analysis of the Commission proposal, argues that the active-passive distinction is illustrative of an underlying and deliberate legislative intent to develop a personal data taxonomy and to create a separation between "received, observed, inferred and predicted data," with only received personal data being considered "a legitimate non-monetary payment for the supply of digital content."[142] It is submitted here, however, that despite being deliberate, rather than representing an informed legislative choice, the proposal instead manifests the complex legislative history related to the attempted harmonization of contract law formation at the EU level and an apparent disregard for the nuances in data protection and privacy. The EDPS was particularly strong in his criticism of the Commission draft, the EDPS proposes the use of the notion of services as defined in the Treaties to encompass services where no price is paid. To clarify, in the ISS context the e-Commerce Directive includes services financed by advertising,[143] and the Court of Justice has found that services as defined by Article 57 TFEU do not necessarily require payment by the users.[144] As a second, but inherently linked alternative, the EDPS suggested that one could refer to Article 3(2)(a) GDPR, which specifies the territorial scope in the GDPR, by stipulating that the GDPR applies where personal data are processed in "the offering of goods or services, irrespective of whether a payment of the data subject is required."[145]

Nevertheless, despite the EDPS's suggestions, there is somewhat of a question mark surrounding whether a service, as defined in either the GDPR, e-Commerce Directive, or the TFEU, may be deemed distinct from a service contract.[146] To clarify, a service contract is defined in Article 2(6) of the Consumer Rights Directive (CR Directive) as "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."[147] In interpreting the scope of the Directive broadly and seemingly in line with Article 57 TFEU, DG Justice has stated in its interpretative guidance of the CR Directive that such contracts do not require the payment of

[140]European Data Protection Board, *Opinion 5/2019 on the Interplay between the EPrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities* (Mar. 12, 2019).

[141]For a description, see Zuiderveen Borgesius, *supra* note 13; Clifford, *supra* note 17.

[142]Malgieri, *supra* note 134, at 8–12.

[143]*See* Directive 2000/31, 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 (']Directive on electronic commerce), Recital 18, 2000 O.J. (L 178) 1.

[144]*See* Case C–155/73, Giuseppe Sacchi (Apr. 30, 1974), http://curia.europa.eu/; Case C-352/85, Bond van Adverteerders and others v. The Netherlands (Apr. 26, 1988), http://curia.europa.eu/.

[145]*See* GDPR, *supra* 5, at art. 3(2)(a).

[146]Ellen Wauters et al., *Towards a Better Protection of Social Media Users: A Legal Perspective on the Terms of Use of Social Networking Sites*, 22 Int'l J. L. & Info. Tech. 254 (2014).

[147]Directive 2011/83, 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, 2011 O.J. (L 304) 64, art. 2(6).

المنارة للاستشارات
www.

a price by the consumer, but that accessing online services without the express contractual agreement of individuals is excluded from its scope.[148] Hence, as noted by Helberger, Borgesius, and Reyna, "contracts [for the supply of digital content in exchange of data] that are concluded by tacit agreement would escape the application of the Consumer Rights Directive."[149] As pointed to above, this is undoubtedly the root of the confusion and is illustrative of the clear differences between the data protection and privacy, and consumer protection policy agendas. In simple terms, EU consumer protection, as illustrated by the interpretation given to the CR Directive, draws a distinction between express and tacit agreement which simply does not exist in the data protection and privacy framework.

In essence, therefore, it appears that the differentiation between types of personal data or in the Commission proposal—active and passive collection—may stem from the fact that there is uncertainty as to whether a contractual agreement can be formed under all respective Member State contract law traditions in situations where only such passive data are collected. Indeed, from a common law perspective, given the need for consideration for a valid contract formation, it is unclear whether, for instance, browse-wrap contracts necessarily form a valid B2 C consumer contract—unless personal data is considered consideration. As described above, however, one must question how this interpretation aligns with Article 5(3) ePrivacy Directive and the requirement for consent for the storing or accessing of information already stored on the terminal equipment of a user, like cookies, as defined in the GDPR. In simple terms, it is the same consent that will be used to legitimize the provision of both types of personal data, and accordingly, it is difficult to imagine how such a delineation could be justified.

Furthermore, given the intended strength of the definition of consent in the GDPR, it would seem unlikely that this could be positioned as tacit. Indeed, as outlined above in Section B(II), consent as defined in Article 4(11) GDPR requires a "freely given, specific, informed and unambiguous indication of the data subject's wishes by. .. a statement *or by a clear affirmative action*, [signifying] agreement to the processing of [their] personal data."[150] Irrespective of such nuancing however, when combined with the conditions for consent in Article 7 GDPR as outlined above, one must question how the delineation between forms of data provision could be deemed in line with the GDPR and ePrivacy Directive requirements.[151] It is perhaps with this criticism in mind that the Compromise Directive focuses instead on types of personal data. Despite the above the Compromise version de facto retains the distinction and therefore, there is a large degree of uncertainty as to how all this fits together.

2. Counter-Performance or De Facto Counter-Performance

Aside from the confusion surrounding the differentiation between the passive and active personal data provision, albeit undoubtedly connected, there are also clear difficulties with the provision of personal data for access to a service and thus the controversy stemming from the inclusion of the notion of counter-performance in the Commission proposal. In particular, the EDPS highlighted three concerns associated with the use of the term counter-performance. First, the Commission proposal failed to define the term and that the use of one simple catch-all term appears to oversimplify a variety of business models and data usages. Second, linking the active provision

[148] *DG Justice Guidance Document Concerning 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*, EUROPEAN COMMISSION 64 (June 2014), 2014), https://www.cr-online.de/crd_guidance_en.pdf.

[149] Helberger, *supra* note 84, at 1444.

[150] GDPR, *supra* note 5, at art. 4 (11) (emphasis added).

[151] For a similar discussion of these issues, see Romain Robert & Lara Smit, *The Proposal for a Directive on Digital Content: A Complex Relationship with Data Protection Law*, 19 ERA FORUM 159, http://link.springer.com/10.1007/s12027-018-0506-7 accessed July 6, 2018.

المنارة للاستشارات
www.

of data with the paying of a monetary price is misleading as consumers are often unaware of what they are giving away when it comes to data, and this is not helped by the use of vague and elastic terms to describe the use of the collected data. Third, data and money are clearly not identical, as providing personal data does not deprive an individual of using this same data repeatedly and this complicates matters when it comes to restitution.[152] Thus, expressly recognizing personal data as counter-performance is controversial from a data protection perspective, because from a normative perspective there are no proprietary rights in personal data.[153]

Although the final Compromise deletes the references to the term "counter-performance," potential concerns remain, given that the Directive now *de facto* appears to retain such a role for personal data. The final Compromise stipulates that the Directive applies where the consumer provides or undertakes to provide personal data to the trader. This language appears to have been inspired by the Parliament and Council versions. In particular, the Parliament draft of Article 3(1) stipulated that the Directive:

> [S]hall apply to any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer whether through the payment of a price *or under the condition that personal data is provided by the consumer or collected by the trader or a third party in the interest of the trader.*[154]

Indeed, at first glance this draft provision seemingly did away with the notion of counter-performance by stating that the proposed Directive applied when access to digital content or a digital service is conditional upon on the provision of personal data. It is argued here however, that the Parliament's proposed amendments instead merely presented a more subtle recognition of personal data as a *de facto* quasi-price. This interpretation is further supported when one compares Recital 13 of the Commission draft with the modifications to this provision proposed by the Parliament, see Figure 5 below.

When compared to the Commission version, the Parliament's proposed modifications of Recital 13 reveal that the omission of the term "counter-performance" in its draft Article 3(1), merely implicitly recognized the same role. In short, the Parliament's approach instead acknowledged such a status for personal data by recognizing that access to digital content and services can be conditional upon the provision of personal data. This is evidenced by the retention of the term counter-performance in the Parliament draft of Recital 13, as illustrated in Figure 5 above.

The Council's proposed modifications of Article 3(1) presented another variation, but in essence reflect the underlying intention made apparent from the above discussion of the Parliament amendments. More specifically, the Council version of Article 3(1) stated that:

> [T]his Directive shall apply to any contract where the supplier supplies or undertakes to supply digital content or a digital service to the consumer. ..
>
> *It shall not apply.* .. to the supply of digital content or a digital service for which the consumer does not pay or undertake to pay a price and *does not provide or undertake to provide personal data to the supplier.*

[152] *Opinion on the Proposal for a Directive on Certain Aspects, supra* note 121. For a discussion of the EDPS criticisms of the concept of counter-performance, see Robert & Smit, *supra* note 151.

[153] Maurizio Borghi et al., *Online Data Processing Consent under EU Law: A Theoretical Framework and Empirical Evidence from the UK*, 21 Int'l J. of L. & Info. Tech. 109, http://ijlit.oxfordjournals.org/content/early/2013/03/09/ ijlit.eat001.

[154] Digital Content Directive (Parliament draft), *supra 125*, at Article 3(1). (emphasis added).

المنارة للاستشارات
www.

PROPOSED DIGITAL CONTENT DIRECTIVE – RECITAL 13	
COMMISSION PROPOSAL	In the digital economy, information about individuals is often and increasingly seen by market participants as having a value comparable to money. Digital content ***is*** often supplied not in exchange for a price but against ***counter-performance other than money*** i.e. by giving access to personal data or other data. Those specific business models apply in different forms in a considerable part of the market. Introducing a differentiation depending on the nature of the counter-performance would discriminate between different business models***; it would provide*** an unjustified incentive for businesses to move towards offering digital content against data. ***A level playing field should be ensured.*** In addition, defects of the performance features of the digital content supplied against ***counter-performance other than money*** may have an impact on the economic interests of consumers. ***Therefore*** the applicability of the rules of this Directive should not depend on whether a price is paid for the specific digital content in question.
PROPOSED PARLIAMENT AMENDMENTS	In the digital economy, information about individuals is often and increasingly seen by market participants as having a value comparable to money. Digital content ***and digital services are*** often supplied not in exchange for a price but against ***data,*** i.e. by giving access to personal data or other data. Those specific business models apply in different forms in a considerable part of the market. Introducing a differentiation depending on the nature of the ***counter-performance*** would discriminate between different business models, ***which provides*** an unjustified incentive for businesses to move towards offering digital content ***or digital services*** against data. In addition, defects of the performance features of the digital content ***or digital service*** supplied against ***data as counter-performance*** may have an impact on the economic interests of consumers. ***In order to ensure a level playing-field,*** the applicability of the rules of this Directive should not depend on whether a price is paid for the specific digital content ***or digital service*** in question.

Figure 5.

> It shall also not apply where personal data are exclusively processed by the supplier for supplying the digital content or digital service, or for the supplier to comply with legal requirements to which the supplier is subject, and the supplier does not process these data otherwise.[155]

As such, the Council modifications replaced the notion of counter-performance and instead framed the role of the provision of personal data in negative terms. More simply, according to the Council version, the Directive does not apply if the consumer does not provide or undertake to provide personal data. This is in contrast to the Commission text that recognized the notion of counter-performance, and the Parliament amendments which provided for situations in which traders give access to digital content or services to consumers either through "the payment of a price or under the condition that personal data is provided."[156] Thus, although the Council amendments certainly reflected the discussion above in relation to the acknowledgement of personal data as *de facto* counter-performance, they also appear to indicative of the Member State reticence in relation to any attempt to harmonize contract law formation at the EU level. Indeed, the Council construction of the provision, in addition to their intention to retain the passive-active distinction, revealed the fear that a positive acknowledgement of personal data as counter-performance in an EU legislative text, even if implicit, would have had an impact on this tightly guarded aspect of national contract law. This is evident in footnote 15 of the Council's general approach which included the specification that the contractual protections in its version of the proposed Directive can be extended to situations where only passive data are provided where this is considered a contract by national law.[157] Importantly, the concerns manifested in the Commission and Parliament versions are reflected in the final Compromise.

[155]Digital Content Directive (Council draft), *supra* 126, at art. 3(1).
[156]Digital Content Directive (Parliament draft), *supra 125*, at art. 3(1).
[157]Digital Content Directive (Council draft), supra 126, at footnote 15.

المنارة للاستشارات
www.

The Compromise version tries to create a clear delineation between contracts supplied for a price versus those created where the consumer provides personal data. There is some very careful wording in the Compromise in comparison to the Commission proposal incorporating the concerns associated with recognising personal data as an economic asset to be bartered and traded and thus the Council and Parliament versions. Here reference can be made to Recital 13 Digital Content Directive (Compromise) which states inter alia that, "[w]hile fully recognising that the protection of personal data is a fundamental right and therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are in the context of such business models entitled to contractual remedies."[158] In other words, therefore although personal data cannot be considered as a commodity, the provision of personal data can give rise to a contract with the consent of the consumer-data subject—provided the other requirements on contract law formation in national law are met—giving rise to a consumer contract.[159]

For instance, from a common law perspective recognizing that the provision of personal data gives rise to a contract could essentially lead to the personal data being regarded as *sufficient* consideration.[160] Therefore, although the use of the term counter-performance attracted much ire, it is perhaps the underlying recognition of the economic value of personal data vis-à-vis contract formation which is the more apt target for such a debate. Somewhat counterintuitively, therefore, data protection enthusiasts critical of positioning personal data as a quasi-price may find support in those critical of contract law formation harmonization. Indeed, as noted by Mak, an important doctrinal question in this regard therefore, is how this provision of personal data will give rise to a contract in national law.[161] The author goes on to specify that this presents important challenges as *inter alia* most national contract laws require a monetary payment for a sales/services contract.This matter is far from clear-cut, and although the analysis may seem somewhat tangential to our current focus, the UCT Directive inherently assumes that in the operation of its provisions some price and consideration will be paid—as evidenced by the exclusion of such core terms from the substantive fairness element in the Directive. As a consequence, the determination of what the price is in relation to declarations of consent is an issue worthy of discussion, as it will effectively determine what is exempt. Therefore, the classification of personal data as a price is of key importance to the operation of the UCT Directive, and subsequently, the substantive fairness element contained therein.

II. Data, Price, and Contract Versus Consent

The analysis in the previous sub-Section has revealed a number of questions in relation to the overlaps between contract law and consent, contract, and legitimate interests as conditions for lawful processing in the GDPR. Indeed, given that personal data processing necessary for the provision of the service is deliberately excluded from Digital Content Directive (Compromise), one must question in particular the relationship between consent in Article 6(1)(a) GDPR and

[158]Digital Content Directive (Compromise), *supra* 117, at recital 13.

[159]As opposed to any of the other conditions for lawful processing contained in Article 6(1)GDPR. This is manifested in two ways. First, the use of the phrasing 'the consumer provides or undertakes to provide personal data' which seemingly excludes processing based on Article 6(1)(f) GDPR (legitimate interest) from triggering a contract and second, the apparent exclusion of other 'necessary' processing. More specifically, as alluded to in Article 3(1) Digital Content Directive (Compromise) and Article 3(4) of the Commission proposal, the Directive does not apply where the processing of personal data is exclusively required to supply the digital content or service or to comply with a legal obligation provided 'the trader does not process this data for any other purpose.' This specification, therefore, excludes processing based on Article 6(1)(b) GDPR and Article 6(1)(c) GDPR from the scope of protection.

[160]In general, consideration for a contract must be sufficient, but it need not be adequate. *See White v. Bluett* [1853] 23 LJ Ex 36.

[161]Vanessa Mak, *Contract and Consumer Law*, *in* Research Handbook in Data Sci. & L. 17, 33-34 (Vanessa Mak et al., 2018).

المنارة للاستشارات
www.

contract in a consumer law sense. More specifically, one must question whether consent to personal data processing then necessarily results in a contractual agreement within the operation of the Compromise Directive. With this in mind, how the overlaps between contract as a condition for lawful processing in Article 6(1)(b) GDPR and consent in Article 6(1)(a) GDPR, as well as how the UCT Directive, and more specifically, the protection against unfair pre-formulated declarations of data subject consent fit within this complex interwoven legal framework can also be questioned.

1. Necessity and the Role of Consent

Building on the above, it is important to remember Article 7(2) GDPR laying down the requirement that consent must be presented in a manner which is clearly distinguishable from the other matters, and Article 4(11) GDPR which stipulates that consent must be freely given. The requirement for the separation of consent and other matters is reinforced in Article 7(4) GDPR which states that:

> [W]hen 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.[162] [Emphasis added]

As noted by the EDPS, this separation is further evident in Recital 43 GDPR which provides that where "the performance of a contract, including the provision of a service, is dependent on . . . consent despite such consent not being necessary for such performance," there is a presumption that consent is not freely given.[163]

In analyzing these provisions, one must wonder what this separation of consent and other matters—for example, the details of the contract—means from a theoretical perspective regarding the classification of the pre-formulated declaration of consent subject to the contractual protections afforded by the UCT Directive. If consent is to be separated from the provision of the service, how can the GDPR rely on the application of the protections against unfair terms in pre-formulated declarations of consent in its recitals if personal data is to be viewed as the price for the provision of the service? In other words, as consent precisely constitutes a lawful condition for the processing of an individual's personal data and the personal data would at the same time constitute the *de facto* price for the provision of the service to the individual in a B2 C consumer contract sense, it seems at first glance to be counterintuitive to present consent in a manner which is clearly distinguishable from the other matters as required by Article 7(2) GDPR. This challenge manifests itself even more clearly when one recognizes the distinction between consent and contract as conditions for lawful processing.

Article 6(1)(b) GDPR provides that personal data processing is lawful where such "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."[164] Importantly, the notion of necessity has its own distinct meaning within the scope of the GDPR. In essence, this refers to the necessity component in the fair balancing element of the fairness principle in data protection. The question thus becomes what is necessary for the performance of a contract and hence, the argumentation around whether—and, if so, which—personal data processing operations are integral to the delivery of free services and the economic underpinnings of the internet. The Article 29 Working Party has repeatedly noted that it seems unlikely that large scale personal data processing for commercial purposes—for example, online behavioral advertising—would satisfy

[162]GDPR, *supra* note 5, at art. 7(4) (emphasis added).
[163]*Opinion on the Proposal for a Directive on Certain Aspects, supra* note 121, at 18.
[164]*See* GDPR, *supra* 5, at art. 6(1)(b).

المنارة للاستشارات
www.

this necessity test.[165] There is therefore a distinction between consent and contract as conditions for lawful processing but what does this mean in terms of the conditionality of consent and thus the relationship between consent and consumer?

Here it is important to note that the Working Party has explicitly stated "the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract."[166] Despite the fact that this is an ongoing debate, from a systematic reading of the GDPR it is indeed difficult to position personal data as a price. Such doubt also appears to reflect a teleological interpretation of the GDPR in that although the Regulation has dualist aims—for example, as it also focuses on the integration of the internal market—it is more predominantly weighted towards the protection of fundamental rights and freedoms and in particular, the right to data protection—as evidenced by its reliance on Article 16 TFEU as its legislative basis. Indeed, if one was to position personal data as the core term, how would this align to the fair balancing, and hence, the proportionality and necessity components? More specifically, the very purpose of Article 4(2) UCT Directive is to leave such matters for the contractual parties. Although data protection is not an absolute right, it nevertheless establishes key fairness checks and balances in the GDPR which must be respected.

Nevertheless, as the recent policy initiatives show, this matter is far from simple to understand. In this regard one must wonder how the Article 29 Working Party opinion on consent aligns for instance with the modifications of the consumer law *acquis*. How can the Article 29 Working Party issue an opinion that appears to contradict the Digital Content Directive Compromise and the new deal for consumers? And, therefore, should the freely given stipulation be understood not as a strict requirement, but instead merely as an indicator that utmost account shall be taken of whether access to the service is conditional on consent? An important point of reference here is the recent opinion by Advocate General Szpunar in the Planet 49 case where he notes that "[. . .] from the terms 'utmost account shall be taken of', the prohibition on bundling is not absolute in nature."[167] There is clearly a large degree of uncertainty here as to how these provisions and frameworks are to be interpreted. Hence, it remains to be seen not only how far consent will be stretched, but also how processing that is necessary for the contract will be delineated from additional activities. The Digital Content Directive as a legislative development, provided it is formally published in the Official Journal, should therefore be considered to have more authority than the non-legally binding opinions of the Article 29 Working Party. Ultimately, the boundaries of the notion of consent will need to be determined by the Court of Justice.[168] Hence, the classification of what constitutes the core terms for the purposes of the UCT Directive remains uncertain, and this is indicative of the teething problems inherent to the alignment of the data protection and consumer protection policy agendas. This uncertainty illustrates the fundamental divide between the dominant view in data protection, which positions personal data protection as a fundamental right, and the approach in consumer protection and competition law which are increasingly recognizing and catering to the economic value of personal data.[169] Although the

[165]Opinion 06/2014, *supra* note 32; Opinion on Online Behavioural Advertising, *supra* note 34.

[166]*Id.* at 8; *see also* European Data Protection Board, *Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects* (Apr. 9, 2019).

[167]Opinion of Advocate General Szpunar delivered on 21 March 2019 in Case C-673/17 Planet49, para. 98 (Mar. 21, 2019) http://curia.europa.eu/.

[168]In this regard, it is instructive to note that the Court of Justice has continuously expanded personal data protection in recent judgments. For a discussion on the change in how the Court has dealt with data protection since the adoption of the Lisbon Treaty and the entry into force of the Charter of Fundamental Rights of the European Union, see Orla Lynskey, *From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis*, *in* EUR. DATA PROTECTION: COMING OF AGE (Serge Gutwirth et al., 2013), http://link.springer.com/chapter/10.1007/978-94-007-5170-5_3. For a critical analysis of the expansion of what is meant personal data, see Nadezhda Purtova, *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, 10 L., INNOVATION AND TECH. 40 (2018).

[169]In the competition law context, see, for instance, the statement of Competition Commissioner Vestager:

المنارة للاستشارات
www.

ability to offer higher levels of protection also extends to the exclusion of the exemption provided in Article 4(2) UCT Directive in the national implementation,[170] legal certainty and a fully harmonized approach appear to be at risk. In this regard it is important to remember that Recital 42 GDPR refers to pre-formulated declarations of consent specifically.

2. Positioning Consent and Applying Contractual Protections

Although it is clear from the above analysis that consent and contract are separate and entirely distinct conditions for lawful processing in the GDPR, this separation raises some doubt as to the positioning of consent in relation to the contractual protections in the UCT Directive. In other words, can consent to a pre-formulated declaration be understood as a contract in its own right despite its required separation from the provision of a service contract? Can consent in Article 6(1)(a) GDPR itself be reduced to a form of contract? And can consent to a pre-formulated declaration legitimizing personal data processing in effect act as a trigger for the formation of a B2 C consumer contract?

In responding to these complex questions, one must remember that it remains uncertain as to whether the separation of consent and contract in Article 7(4) GDPR is merely potentially indicative of a scenario in which the freely given stipulation may be infringed and, hence, whether it in fact gives rise to a rebuttable presumption and does not entirely delegitimize rendering access to a service conditional upon the provision of personal data. Indeed, despite the Article 29 Working Party Opinion, this remains a matter for the Court of Justice to decide. It is thus arguable that privacy policies in addition to terms of use should be presented as the provisions of the contract with the declaration of consent being a separate, and, indeed, revocable but connected part of the same overarching contractual agreement, despite the presumption and associated burden of proof. With this in mind, personal data does not necessarily have to constitute a price, but the protection of it may be encompassed within the contractual agreement as both explicit[171] and implied terms.[172] Currently interpreting where personal data fits is a matter for national contract law and national courts.

This interpretation does not, however, render contract and consent synonymous—as contract law assumes the autonomous decision making capacity of individuals. Therefore, although the formation of a contract requires the voluntary assent of the parties, consent in data protection

---

Consumers use search engines that produce incredibly accurate results. Social networks let people keep in touch with friends, wherever they are in the world. And they don't pay a single penny for those services. Instead, they pay with their data. That doesn't have to be a problem, as long as people are happy that the data they share is a fair price to pay for the services they get in return. Personal data has become a valuable commodity.

Margrethe Vestager, Commissioner for Competition, Data Ethics event on Data as Power in Copenhagen: Making Data Work for Us (Sep. 6, 2016), https://ec.europa.eu/commission/commissioners/20142019/vestager/ announcements/making-data-work-us_en.

[170] *See* Caja de Ahorros y Monte de Piedad de Madrid, *supra* note 106.

[171] For example, what the controller promises.

[172] For example, legal obligations stemming from the GDPR. But what else, then, could be classified as the price? Despite the fact that, in the context of SNS, the provision of content by the data subject may constitute consideration, not all ISS incorporate the use of user generated content. More specifically, although, in the context of social networking sites one could argue that the content—for example, text, photos, videos.—provided by the user could be considered a price, the argumentation becomes far murkier where the user engages with the services without providing such content—for example, a search engine—unless search queries would qualify. On the contrary, the viewing of advertisements—whether in addition to the provision of user generated content or not—can be regarded as the price for the purposes of Article 4(2) UCT Directive. From a competition law perspective, reference can be made here to the positioning of attention as a parameter on the basis of which market players compete in multi-sided markets where "online attention rivals provide products and features to obtain the attention of consumers and sell some of that attention, through other products and services, to merchants, developers, and others who value it." David S. Evans, *Attention Rivalry among Online Platforms*, 9 J. OF COMPETITION L. & ECON. 313, 313 (2013).

المنارة للاستشارات
www.

cannot be reduced to a form of contract, given that it must not always be freely given, specific, informed, and unambiguous as understood under the GDPR, in order for it to be considered a B2 C contract. This is indicative of the fact that the UCT Directive focuses on the fairness of the terms themselves and explicitly excludes the analysis of the validity of the contract formation. As such, the validity of a data subject's consent and the fairness of the pre-formulated declaration of consent are two connected, but distinct, issues. Nevertheless, this higher threshold for consent in data protection does not exclude the possibility that the data subject's consent may give rise to a B2 C contract. Indeed, this currently hinges on whether the provision of personal data can be recognized as conditional for the provision of the service in national contract law, or indeed on whether national contract law otherwise recognizes the existence of a B2 C contract.[173] The Article 29 Working Party opinion should therefore be taken with a grain of salt, as this is an issue which is far from resolved. As such, much hinges on the interpretation of the Digital Content Directive (Compromise) and Article 7 GDPR by the Court of Justice, as well as the reform of the ePrivacy Directive and therefore the proposed ePrivacy Regulation.

To illustrate, one can refer here to the debate surrounding the legitimacy of cookie walls in the discussion surrounding the proposed ePrivacy Regulation. More specifically, as outlined above in Section D(I)(1), Article 5(3) ePrivacy Directive requires consent for the "storing of information, or the gaining of access to information already stored, in the terminal equipment" of the user.[174] There are ongoing debates as to whether there should be a ban on cookies walls—such as cookie notices which require you to accept the use of cookies in order to access the service—as these effectively render access to the service conditional upon consent with the EDPS, and others criticizing the failure to include a specific ban on the use of cookie walls.[175] Following this criticism, the European Parliament draft[176] introduced a ban on the use of cookie walls.[177] But, the Council's consolidated approach, released on December 5th, 2017, did not follow this example.[178] As such, it remains largely uncertain how this will be resolved and the various rumblings which have emerged since the release of the two drafts referred to above indicate that this is still a very sticky issue. Indeed, in this regard it is important to note that the reform of the

[173] *See* Mak, *supra* note 161.

[174] As described by the Article 29 Working Party, Article 5(3) ePrivacy Directive allows for processing to be exempt from the requirement of consent if one of the following criteria is satisfied: (1) Technical storage or access "for the sole purpose of carrying out the transmission of a communication over an electronic communications network"; or (2) technical storage or access which is "strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service." *See* Opinion 04/2012, *supra* note 139.

[175] *Preliminary EDPS Opinion on the Review of the EPrivacy Directive (2002/58/EC)*, EUR. DATA PROTECTION SUPERVISOR (July 22, 2016), https://edps.europa.eu/sites/edp/files/publication/16-07-22_opinion_ eprivacy_en.pdf; Article 29 Working Party, *Opinion 01/2017 on the Proposed Regulation for the EPrivacy Regulation (2002/58/EC)*, WP 247 (Apr. 4, 2017). In the proposed reforms of the ePrivacy Directive, the proposed ePrivacy Regulation—largely speaking—retains the general rule in Article 5(3) ePrivacy Directive. Article 8(1)(d) of the proposed Regulation adds an additional ground for processing in comparison to the ePrivacy Directive. More specifically, the activities referenced above in Article 8(1) shall be permitted "if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user." Accordingly, instead of providing a general consent rule with the two exemptions for functional cookies, the proposed Regulation includes this additional grounds for web audience measurement.

[176] *See* "Stronger Privacy Rules for Online Communications," EUR. PARL. (October 19, 2017) http://www.europarl.europa.eu/news/en/press-room/20171016IPR86162/stronger-privacy-rules-for-online-communications.

[177] *See Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, at art. 8(1)(a) (Oct. 20, 2017), http://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html.

[178] *European Council Draft Text, Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, COUNCIL OF THE EUROPEAN UNION (Dec. 5, 2017), http://data.consilium.europa.eu/doc/document/ST-15333-2017-INIT/en/pdf.

المنارة للاستشارات
www.

ePrivacy Directive as a *lex specialis* framework could essentially decide the conditional consent debate and provide the practical interpretation for the GDPR. To clarify, given that cookies are considered personal data and are effectively a key means through which personal data is gathered in an ISS context, a failure to ban cookie walls, or indeed the provision of a partial ban in the *lex specialis* rules, would seemingly legitimize the use of such technologies by omission—at least in certain circumstances.[179]

From the above, therefore, although the legislator intended to cross-reference the protections in the UCT Directive in Recital 42 GDPR for pre-formulated declarations of consent, there are many unresolved issues centered around the recognition of the economic value of personal data. Despite the fact that the EDPS and Article 29 Working Party have criticized the positioning of personal data as a form of payment, this remains a highly contentious issue with divergences in interpretation amongst policy makers, academics, and even different enforcement bodies.[180] Indeed, at first glance, it seems unlikely from a systematic and teleological interpretation of the GDPR that personal data could be positioned as the price, given the separation of data subject consent from other matters in order to be certain that it will not fall foul of the freely given requirement; despite this fact, this position has not been reflected in consumer protection and competition law and policy. The uncertainty regarding the recognition of the economic value of personal data described above raises a number of issues in terms of how the GDPR may be interpreted in practice and by the Court, in particular in light of the Digital Content Directive (Compromise). One must therefore wonder whether the Article 29 Working Party opinion on consent is truly sustainable in the current regulatory environment. The action taken by Max Schrems referred to in the introduction will hopefully provide the answer to this question, however, one must wonder whether a more tiered understanding of conditionality is in fact needed.

E. Data Protection and Freely Given Consent—A Framework Designed to Counteract Imbalances?

In his preliminary opinion on the reform of the ePrivacy Directive, before the publication of the Commission proposal, the EDPS recommended that the legislator consider a complete or at least a partial ban on the use of cookies walls.[181] The purpose of this next Section, therefore, is to more thoroughly examine what is meant by a freely given indication of the data subject's wishes with a more tiered or graduated understanding of conditionality in mind. In essence, the analysis will examine if data subject consent may be conditional for the provision of a service contract without falling foul of the freely given stipulation in the definition of consent in Article 4(11) GDPR more generally, with reference to competition law. Thus, the analysis will examine how conditional access to content or service, as provided for in the Digital Content Directive (Compromise), actually fits within the GDPR notwithstanding the strict interpretation in the Article 29 Working Party opinion.

[179] *See* Frederik J. Zuiderveen Borgesius et al., *Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the EPrivacy Regulation*, 3 EUR. DATA PROTECTION L. REV. 353 (2017).

[180] For instance, in this regard, it is important to note that, although consumer protection agencies—as illustrated by the common position and the AGCM and Federation of German Consumer Organizations interpretations—recognize the economic value of personal data, the Berlin Regional Court recently found that intangible consideration could not be considered as a cost, and, accordingly, Facebook is not barred from advertising itself as free. *See* Landgericht Berlin [LG Berlin] [Berlin Regional Court] Jan. 1, 2018, 16 O 341/15; *see also Facebook Verstößt Gegen Deutsches Datenschutzrecht*, VERBRAUCHERZENTRALE BUNDERESVESBAND (Feb. 12, 2018), https://www.vzbv.de/pressemitteilung/facebook-verstoesst-gegen-deutsches-datenschutzrecht.

[181] *Preliminary EDPS Opinion on the Review of the EPrivacy Directive*, *supra* note 175, at 15.

المنارة للاستشارات
www.

I. Take It or Leave It Choices and Freely Given Consent

Where consumers are confronted with take-it-or-leave-it offers and do not have a real choice but to accept the terms and conditions if they want to use a particular service, it seems difficult to ensure that consent is freely given. It is seemingly on this basis that the Article 29 Working Party has drawn a strict line dividing processing necessary for the provision of a service, and other processing requiring consent, in its interpretation of Article 7(4) and Recital 43 GDPR. Due to the existence of economic characteristics such as network effects, economies of scale and economies of scope, the markets in which online businesses compete are typically characterized by the presence of only a few firms that have a rather large market share. Individual control over personal data is becoming illusory when dominant companies are able to impose their practices on individuals by exploiting their strong position. This may result in an imbalance of power between individuals and providers of online services, which calls into question the existence of a genuine choice for data subjects as to whether or not to give their consent to a particular form of personal data processing.[182] As such, one can question the appropriateness of consent as a condition for lawful processing where only a limited number of providers are present in the market or where one provider is dominant.

Recital 43 GDPR makes these issues explicit and provides that consent should not be a valid legal ground where there is a clear imbalance between the data subject and the controller. Although the recital continues by referring, in particular, to the situation where a public authority acts as a controller where "it is therefore unlikely that consent was freely given in all the circumstances of that specific situation,"[183] the described imbalance is not exclusive to situations in which public authorities act as controllers, but is also applicable in the reality of current concentrated online markets.[184] This interpretation of Recital 43 GDPR is supported by both the Article 29 Working Party and the EDPS,[185] and consequently, there appear to be two components to consider in the assessment of the freely given stipulation in this context, namely: (1) An assessment of all the circumstances of that specific situation which is activated only if (2) a clear imbalance exists between the controller and the data subject. The GDPR, therefore, appears to require an assessment of the controller-data subject asymmetry in abstract—for example, in general and not with specific reference to the particular context of the data subject(s)—in order to establish if a clear imbalance exists. Subsequently, an analysis of the established imbalance is needed in order to assess whether the freely given requirement has been violated, or whether it is justifiable in the circumstances of that specific situation. Nevertheless, it is difficult to interpret what these elements may incorporate concretely.

It is suggested here that in keeping with the accountability principle, the controller may be required to prove not only that informed, specific, and unambiguous consent has been provided in line with the requirements in the GDPR, but also that the clear imbalance in power did not affect the consumer-citizen's decision to consent, despite the fact that this consent was required to access the service in question. It is not at all clear what this may mean, given that the GDPR works from the assumption of an asymmetrical controller-data subject relationship and that hence, it is hard to imagine a situation where there would not be an asymmetric controller-data

[182] *Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy*, EUR. DATA PROTECTION SUPERVISOR para. 79 (Mar. 26, 2014), https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_ data_en.pdf

[183] *See* GDPR, *supra* 5, at recital 43.

[184] In the 2012 Commission proposal, Article 7(4) GDPR even stated generally that "[c]onsent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller." *See Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 011 final (Apr. 27, 2016).

[185] *See Opinion Guidelines on Consent under Regulation 2016/679*, *supra* note 62; *Opinion on the Proposal for a Directive on Certain Aspects*, *supra* note 121, at 18.

المنارة للاستشارات
www.

subject relationship, especially in an ISS context. This echoes the point above regarding imbalance and the UCT Directive in Section C(II)(1). With this in mind, one must question what is to be understood by a clear imbalance in practice or in other words, the circumstances in which this presumption of the failure to satisfy the freely given consent stipulation would be rebuttable. Interestingly, in its opinion on consent, the Article 29 Working Party interprets the provisions as precluding a controller from arguing that the data subject's consent was freely given on the ground there is a choice between its services and those of competitors.[186] The Working Party notes that such an interpretation would render the data subject's freedom of choice dependent on: (1) Other market players; (2) whether the data subject actually deemed the services equivalent; and would also (3) require the controller to constantly monitor competitors to ensure the validity of the data subject's consent. This would clearly have an impact on legal certainty.

Nevertheless, given the above policy developments and the uncertainty surrounding the future of the proposed ePrivacy Regulation and indeed the seemingly imminent adoption of the Digital Content Directive (Compromise), it seems that the Working Party's approach may need to be revisited in the future. Indeed, there is an ongoing fundamental debate surrounding the merits of surveillance capitalism[187] and the ongoing legitimacy of the monetization of personal data, as evidenced by the contrast between the reforms and the Working Party's opinion on consent. Do we want to ban business models centered around the monetization of personal data? Or force companies to offer alternative personal data-based and pay-for-access, monetary funded versions of the same service? Personalized advertising is certainly not the only way of monetizing online services. But would the second option not *de facto* also put a price on the rights to data protection and privacy? These are all fundamental and normatively challenging questions which need to be answered. It seems unlikely, however, that the Article 29 Working Party's strict interpretation of consent, and its separation of processing necessary for the provision of the service will be sustainable in light of the various moves to recognize the economic value of personal data and the broader internal market considerations of the EU legislator.

Moreover, although there is strong merit to each of the Working Party's arguments listed above, it is suggested that the only reasonable consequence of failing to engage with the question of the controller's position on the market would be to acknowledge the conditionality-availability distinction between consent and explicit consent implicit. More specifically, if the proposed ePrivacy Regulation is adopted and in keeping with the Digital Content Directive (Compromise) directly or indirectly allows for the rendering of consent to be conditional for access to services, by continuing to refuse to factor in market power in the assessment of the freely given stipulation in the future, the Working Party could conceivably be left with for instance, the delineation of consent and explicit consent as the sole means of assessing conditionality. One might wonder whether such an approach would respect the spirit of the GDPR and the risk-based approach inherent to the interpretation of the Regulation's requirements. In short, the potential legislative recognition of the legitimacy of conditional access based on consent may force the Working Party to reconsider whether Facebook's and other market players' position should be a consideration in the assessment of the validity of consent under the freely given stipulation. Indeed, in this regard, one must question whether smaller market operators should be denied rendering consent conditional where they are merely a minor player on the market. In these circumstances, there is less need for a strict interpretation of consent, as the risk that there is no free choice for data subjects is countered by the presence of other market players to which data subjects can switch. A strict approach may even discourage small businesses and start-ups from entering the market, thereby reducing

[186] *Opinion Guidelines on Consent under Regulation 2016/679*, *supra* note 62, 9–10.

[187] *See* Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75 (2015); Shoshana Zuboff, *Google as a Fortune Teller: The Secrets of Surveillance Capitalism*, FRANKFURTER ALLGEMEINE (March 5, 2016), http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/ shoshana-zuboff-secrets-of-surveillance-capitalism14103616p2.html?printPagedArticle%3dtrue#pageIndex_2.

المنارة للاستشارات
www.

the choice that the Article 29 Working Party in fact aims to protect. Consequently, is this the desirable choice, or could there not be a role for competition law in identifying situations in which the conditionality of access would have an impact on data subject consent?

Data protection advocates have expressed increasing attention in competition enforcement in recent years.[188] These debates have so far mainly addressed the question of how data protection interests can be considered in the competition analysis, and how competition enforcement may thereby strengthen the effectiveness of data protection law. But, the complementarity of the two regimes could also work the other way around.[189] The use of competition principles in data protection law seems particularly promising in the interpretation of the scale of the obligations with which controllers and processors have to be in compliance. Competition concepts of market definition and dominance could play a useful role here; the stronger the position of a controller or processor in the market, the riskier the processing activities for the right to data protection of the individual. It is worth noting in this regard that the GDPR does consider the level of risk of a certain form of processing in such a way that more detailed obligations will apply to controllers where the risk of processing is higher. For example, the risks of varying likelihood and severity for the rights and freedoms of natural persons play a role in determining to what extent the controller must implement appropriate technical and organizational measures to ensure, and be able to demonstrate, that the processing of personal data is performed in compliance with the applicable rules under Article 24(1) GDPR. In a similar vein, the Court of Justice referred to the ubiquity of online search engines in Google Spain when determining the effect of the interference caused by Google's processing of personal data with the fundamental rights to privacy and data protection of the data subject at issue.[190]

Unlike competition law, data protection law is not concerned with scale because a breach of data protection rules can be equally damaging to the interests of individual data subjects irrespective of the market position of the firm and the size of the dataset or the processing activities.[191] Nevertheless, while no formal distinction is made on the basis of scale or size under EU data protection law, the risk inherent in particular processing activities, and the ubiquitous nature of a controller, can thus be considered as relevant factors in establishing, respectively, the scale of its obligations under the GDPR and the impact of its processing activities on the rights of the data subject. These factors resemble, at least to a certain extent, the well-established principles of market definition and dominance in competition law. In this regard one can refer to a number of examples throughout GDPR in order to highlight the prioritization of risk and, thus, the risk-based regulatory model employed in the Regulation.

[188]The EDPS has been particularly active in stimulating this discussion by publishing two opinions: Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy, March 2014 and Opinion 8/2016 on Coherent Enforcement of Fundamental Rights in the Age of Big Data, September 23, 2016.

[189]For an extensive discussion, see Inge Graef et al., *Fairness and enforcement; bridging competition, data protection, and consumer law*, 8 Int'l Data Privacy L. 200 (2018).

[190]Case C-131/12, Google Spain SL and Google Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, (May 13, 2014), http://curia.europa.eu/.

[191]The GDPR, however, does consider the level of risk of a certain form of processing in such a way that more detailed obligations will apply to controllers where the risk of processing is higher. For example, "the risks of varying likelihood and severity for the rights and freedoms of natural persons" play a role in determining to what extent the controller must implement appropriate technical and organizational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with the applicable rules under Article 24(1) of the GDPR. In addition, the Court of Justice referred to the ubiquity of online search engines in *Google Spain* when determining the effect of the interference caused by Google's processing of personal data with the fundamental rights to privacy and data protection of the data subject at issue. *Id.* While no formal distinction is made on the basis of scale or size under EU data protection law, the risk that particular processing activities may bring about and the ubiquitous nature of a data controller can thus be considered as relevant factors in establishing, respectively, the scale of its obligations under the GDPR and the impact of its processing activities on the rights of the data subject.

المنارة للاستشارات
www.

More specifically, aside from the higher risks and stricter requirements associated with the processing of sensitive personal data and, thus, delineations based on data type, the GDPR also refers to the scale of the processing operations—for instance, in the requirements relating to the appointment of a data protection officer and the exercising of a data protection impact assessment. In short, these provisions reflect the role of the fair balancing element of the GDPR's fairness principle and, thus, the application of the proportionality and necessity principles as components of this element. As a context dependent assessment, competition law analysis could provide valuable insights into the practical application of the fair balancing element via the principles of market definition and dominance. Such considerations can be used to examine the availability and viability of alternative services, and thereby the extent of citizen-consumer decision-making capacity in particular circumstances.

Competition law reasoning could, therefore, be used to interpret key data protection concepts such as fairness and accountability. In this sense, the stronger the position of the controller and, thus, the less chance for data subjects to rely on another controller, the stricter the principles of fairness and accountability would need to be applied to adequately protect the interests of data subjects.[192] With regard to the interpretation of the concept of consent, this logic would imply that the existence of dominance in a competition law sense may act as an indicator challenging the validity of consent as a condition for the processing of personal data. In this vein, one could question whether controllers will be able to differentiate between the services that they offer and hence, whether premium services could be offered to those willing to pay either a monetary fee or with their personal data, or even with both. As a result, one must question how such a requirement would map against existing practice and hence, the likelihood of a strict interpretation. Indeed, in this regard one may wonder how this interpretation would affect the business models of companies such as Google and Facebook, given their strong market position in search, social media and also online advertising. It is therefore uncertain what role the freely given stipulation will play in terms of the initial citizen-consumer sign up and thus the requirement to offer the service with personal data processing limited to only that which is necessary for the performance of the contract for the provision of the service.

Interestingly, the German competition authority, *Bundeskartellamt*, opened an investigation against Facebook in March, 2016,[193] which specifically targets the interaction between market dominance under competition law and the validity of consent under data protection law. In February, 2019, the Bundeskartellamt concluded that Facebook abused its dominant position in the market for social networks by infringing data protection rules. In particular, the Bundeskartellamt prohibited Facebook from combining user data from different sources, except if users voluntarily consent to their data being combined. According to the Bundeskartellamt, Facebook's terms and conditions violate data protection law and thereby also constitute exploitative business terms under the abuse of dominance prohibition of competition law. According to the Bundeskartellamt, it cannot be assumed that users effectively consent to Facebook's collection and use of data from third-party sources in view of its dominant position on the market. In the words of the president of the Bundeskartellamt:

> As a dominant company Facebook is subject to special obligations under competition law. In the operation of its business model the company must take into account that Facebook users practically cannot switch to other social networks. In view of Facebook's superior market

[192] *See also* Zingales, *supra* note 89, at 5–6. Zingales gives a discussion of how two decisions taken by the *Autorità garante della concorrenza e del mercato* (Italian competition and consumer protection authority) in May 2017 imposing a fine of € 3 million on WhatsApp for alleged unfair commercial practices indicate the relevance of competition and data protection considerations in consumer law.

[193] *Bundeskartellamt Initiates Proceeding against Facebook on Suspicion of Having Abused Its Market Power by Infringing Data Protection Rules*, BUNDESKARTELLAMT (March 2, 2016), https://www.bundeskartellamt.de/ SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html.

المنارة للاستشارات
www.

> power, an obligatory tick on the box to agree to the company's terms of use is not an adequate basis for such intensive data processing. The only choice the user has is either to accept the comprehensive combination of data or to refrain from using the social network. In such a difficult situation the user's choice cannot be referred to as voluntary consent.[194]

As a result of the decision of the Bundeskartellamt, Facebook has to restrict its collection and combining of data. Assigning data of Facebook-owned services like WhatsApp and Instagram as well as of third party websites to Facebook user accounts is only possible subject to the voluntary consent of users. If consent is not given, the data has to stay with the respective service and cannot be processed in combination with Facebook data. It is up to Facebook to develop proposals to implement the limitations imposed. With regard to Facebook's future data processing policy, the president of the Bundeskartellamt stated that "we are carrying out what can be seen as an internal divestiture of Facebook's data."[195] And that:

> In future, consumers can prevent Facebook from unrestrictedly collecting and using their data. The previous practice of combining all data in a Facebook user account, practically without any restriction, will now be subject to the voluntary consent given by the users. Voluntary consent means that the use of Facebook's services must not be subject to the users' consent to their data being collected and combined in this way. If users do not consent, Facebook may not exclude them from its services and must refrain from collecting and merging data from different sources.[196]

While the Bundeskartellamt is relying on competition enforcement to address unfair collection and use of personal data by incorporating data protection principles into competition law, its investigation also illustrates the relevance of competition law principles for defining the validity of consent within data protection law. In particular, the reasoning of the Bundeskartellamt may be interpreted as an acknowledgement that the existence of dominance in a competition law sense points to a clear imbalance between the data subject and the controller, resulting in a rebuttable presumption that the data subject's consent has not been freely given.[197] Considering the restrictive nature of the concept of dominance, however, this competition law principle should not be the sole indicator.

II. Freely Given and the Data Necessary for the Provision of a Service

Dominance is defined in case law of the Court of Justice as "a position of economic strength enjoyed by an undertaking which enables it to prevent effective competition being maintained on the relevant market by giving it the power to behave to an appreciable extent independently of its competitors, customers and ultimately of its consumers."[198] Very large market shares are in themselves, and save in exceptional circumstances, evidence of the existence of a dominant position.[199] Other factors that are taken into account in the assessment of dominance include the existence of entry barriers that make it difficult for other companies to access the market. The concept of dominance is thus rather restrictive considering that a company will only be found

[194] *Bundeskartellamt prohibits Facebook from combining user data from different sources*, BUNDESKARTELLAMT (February 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/ 2019/07_02_2019_Facebook.html.

[195] *Id.*

[196] *Id.*

[197] Please note that the full decision of the Bundeskartellamt was not yet published at the time of finalizing this Article.

[198] Case C-27/76, United Brands Company and United Brands Continentaal BV v. Commission of the European Communities Chiquita Bananas, para. 65 (Feb. 14, 1978), http://curia.europa.eu/.

[199] Case C-85/76, Hoffman-La Roche v. Commission, para. 41 (Feb. 14, 1979), http://curia.europa.eu/; Case C-62/86, Akzo Chemie v. Commission, 1991 E.C.R. I-03359 para. 60.

المنارة للاستشارات
www.

dominant when it can behave independently on the market. As a result, a clear imbalance for the purposes of the GDPR may arguably still be present even if no dominance can be established from a competition law perspective. The fact that a company is not dominant should, therefore, not automatically result in the conclusion that there can be no clear imbalance in the relationships with its users. For instance, the presence on the market of three undertakings holding market shares of about thirty percent each will normally preclude any finding of dominance,[200] while such a market structure may still not provide effective alternatives to users if the three undertakings, together capturing ninety percent of the market, each have similar privacy policies in place. Although the presence of dominance in competition law terms arguably obviates the need for an additional consideration of whether there is a clear imbalance, its absence should not preclude such a finding altogether.

Aside from this more macro level market dominance-based argumentation regarding the existence of an imbalance, it is important to reiterate that asymmetries are inherent to the operation and underlying presumption of data protection law. Accordingly, it must be understood that even when there appears to be no clear imbalance between the parties, the validity of the data subject consent may still be questioned and, thus, as reflected in the GDPR, the conditions mentioned in the definition of consent—namely that consent must be freely given, specific, informed, and unambiguous—still need to be satisfied. Hence, although the determination of what a clear imbalance means in practice may incorporate and benefit from a competition law analysis, even in the absence of a clear imbalance the freely given requirement still needs to be satisfied. This is manifested and further reinforced by the burden of proof on controllers to be able to demonstrate valid data subject consent in Article 7(1) GDPR.

The freely given stipulation clearly goes beyond an analysis of market dominance and the availability of choice, even in the above interpretation, but also incorporates an analysis of the ability of the data subject to choose freely—for example, freedom from inter alia any form of intimidation, coercion and or deception.[201] The assessment of the freely given stipulation is, therefore, not only strongly context dependent, but is also tied to the other conditions—specific, informed, and unambiguous—mentioned in the definition of consent.[202] For instance, in interpreting what is meant by the term unambiguous, it is useful to refer to the requirement for controllers to be able to demonstrate that the data subject has in fact consented to the processing of their personal data as mentioned above, for example, Article 7(1) GDPR. Additionally, and through a combined reading of Articles 7(1) and 7(4) GDPR—thus, in light of the freely given stipulation—an unambiguous indication would also seemingly require that any such consent is demonstrably connected to the stated specific purpose and that the data subject is informed prior to the giving of the consent and, thus, any resulting processing, and that this prior information is presented in a "distinguishable. .. intelligible and easily accessible form, using clear and plain language".[203] Indeed, in this regard one can refer to the Article 29 Working Party opinion on consent which clearly specifies that blanket consent which fails to indicate the scope and consequences of the processing clearly would not be considered specific.[204] This reflects

[200]With the exception of cases of collective dominance.

[201]*Opinion Guidelines on Consent under Regulation 2016/679*, *supra* note 62.

[202]It is significant to note that in the reform of the data protection framework, the GDPR introduces an important clarification in the definition of consent. In contrast with the definition in Directive 95/46/EC, the GDPR has added the unambiguous condition directly to the definition contained in Article 4(11) GDPR. Although in Directive 95/46/4 C, the requirement for unambiguous consent appeared in both the operation of consent—as a condition for lawful processing, Article 7(a) Directive 95/46/EC—and in the requirements for data transfers—Article 26(1)(a) Directive 95/46/EC—its separation caused a degree of confusion as it seems to be logically part of any correct interpretation of the notion of consent itself, despite in effect being interpreted in a manner consistent with the GDPR by the Article 29 Working Party. Article 4(11) GDPR has thus clarified this uncertainty with the inclusion of unambiguous as a condition directly in the definition of consent.

[203]*See* GDPR, *supra* 5, at art. 7(2), recital 42.

[204]*Opinion Guidelines on Consent under Regulation 2016/679*, *supra* note 62.

المنارة للاستشارات
www.

the interwoven nature of the conditions and is illustrative of the importance of the transparency principle in the GDPR and its substantive aspect, and is further supplemented by the more formal requirements for prior information in Articles 13 and 14 GDPR in terms of the information to be provided to the data subject before the processing of personal data. In addition to these *ex ante* requirements, one can also refer to the Section 1 Transparency and Modalities in Chapter 3 Rights of the Data Subject of the Regulation.[205] Article 12 GDPR relating to transparent information, communication, and modalities for the exercise of the rights of the data subject, implicitly provides the same distinct manifestations of the transparency principle.[206] As such, the transparency principle manifests both substantive and formal aspects in both an *ex ante* and *ex post* context.

But what does all this effectively mean in practice due to the fallibility of consent? Indeed, given the well-documented failures of consent, one must question how these conditions will be interpreted in practice and how effective they will be despite the changes in the GDPR.[207] To reiterate, it remains to be seen how far consent will stretch, but also if, and how, processing that is necessary for the performance of a contract will be delineated from additional activities as required by Article 7 GDPR, or if in practice personal data will be recognized as a *de facto* price or counter-performance. In practice, it is arguable that the role for the freely given stipulation may most readily find its application in updates to existing terms. Indeed, such a prediction is hardly surprising, and in this regard one can again refer to the fallout from the recent Facebook-WhatsApp merger. Such an assessment, as reflected in the AGCM rulings, may be less of an analysis of the fairness of terms under the UCT Directive, and instead may invoke comparisons with the application of the Unfair Commercial Practices Directive (UCP Directive) vis-à-vis the means through which consent was attained.

Although a thorough examination of the UCP Directive remains outside the scope of this Article, it should be noted that distinguishing where data protection enforcement begins, and consumer protection ends—or vice versa—as well as delineating what warrants a contractual or practice orientated fairness assessment, is highly debatable. It is clear, however, that changes in privacy policies are, and will continue to be, viewed skeptically regarding the validity of data subject consent. Irrespective of the specific issues at the core of that particular case, however, it will also be interesting to see if a similar reasoning may be applied for more general updates without the additional merger element. In this context, one should remember the fall-out from Google's decision to merge its privacy policies for its various services in 2012. But, given the ongoing discussion in the proposed ePrivacy Regulation, the issues remain largely up in the air. This uncertainty is particularly prevalent in the interpretation of when a clear imbalance will occur and thus how the applicability and operation of this rebuttable presumption will work in practice.

[205] *See* GDPR, *supra* 5, at art. 12.

[206] More specifically, the first manifestation is vis-à-vis the information to be provided to the data subject and the cross-reference to the information requirements in Articles 13 and 14 GDPR, and any communication under Articles 15 to 22 and 34 GDPR (Article 12(1) GDPR), any action taken under Articles 15 to 22 GDPR ((Article 12(3) GDPR) or lack thereof (Article 12(4) GDPR). The second manifestation: In terms of the means of delivering such information—and hence, the requirement "for concise, transparent, intelligible and easily accessible form, using clear and plain language" (Article 12(1) GDPR)—this should be completed free of charge except in limited circumstances (Article 12(5) GDPR).Finally, the third manifestation: Standardized icons can be used in order "in an easily visible, intelligible, and clearly legible manner a meaningful overview of the intended processing." GDPR, *supra* 5, at art. 12(7).

[207] Eleni Kosta, Consent in European Data Protection Law (Nijhoff Studies, 2013); Paul Bernal, Internet Privacy Rights: Rights to Protect Autonomy (Cambridge Univ. Press, 2014); Christophe Lazaro & Daniel Le Métayer, *Control over Personal Data: True Remedy or Fairytale?*, 12 SCRIPTed (2015), http://script-ed.org/?p%3d1927; Orla Lynskey, The Foundations of EU Data Protection *Law* 229–53 (Oxford Univ. Press, 2016).

المنارة للاستشارات
www.

F. Conclusion

Pre-formulated declarations of consent should respect the data subject interests and, therefore, follow the reasonable expectation that these texts should be drafted with the balancing of interests in mind. In simple terms, privacy policies and pre-formulated declarations of consent should live up to their name and, in essence, respect the data protection fairness principle. This view of the role of pre-formulated terms is far from the practical reality, which raises clear concerns regarding the protection of the right to data protection and its underlying rationales of autonomy and informational self-determination as protected in the GDPR in an effort to tackle informational power asymmetries.[208] In response to this divergence between the law on the books and the law in practice, there has been an increasing use of the UCT Directive in the assessment of terms relating to the processing of personal data. This is also reflected in the GDPR, with Recital 42 GDPR specifically referencing the UCT Directive regarding pre-formulated declarations of consent. The precise contours of the relationship between the GDPR and UCT Directive are uncertain given that, first, the GDPR is an omnibus regime, whereas the UCT Directive refers specifically to B2 C contractual agreements only—for example, consent in the GDPR applies to much more than just B2 C contexts—, and, second, the UCT Directive represents a far more economic assessment as opposed to the fundamental rights approach evidenced in the GDPR.

Despite these differences, however, Benöhr contends more generally speaking that the consumer protection agenda may be furthered by a broad range of Charter rights, including for instance the right to data protection.[209] This appears consistent with the aim of integrating consumer interests in all relevant policies and the goal of targeting more systematic consumer protection as expressed in the European Consumer Agenda in 2012.[210] As such, it is arguable that the adoption of the Charter may breathe new life into consumer protection policy.[211] That said, there are major issues which need to be ironed out.[212] As illustrated in this Article, key challenges await from both a perspective of consumer contract formation as well as a data protection and privacy view. These difficulties are most aptly illustrated in the debates surrounding the recognition of personal data's economic value, and this is clearly a polarizing debate. The legislator seems set on ploughing ahead with maximum harmonization law-making, however. Indeed, due to its apparent failure to approach such issues with true regard for all relevant policy agendas, it is unclear how the Digital Content Directive (Compromise) will be interpreted following its publication in the official journal and the passing of the 2 year transition period, and what this will mean for the data protection and privacy framework. Irrespective of such concerns, however, there is a willingness in consumer protection and competition law circles to recognize the economic value of personal data in contrast to the opinion of the Article 29 Working Party.

That said, the data protection and privacy community is increasingly turning towards consumer protection and competition law to help provide more holistic citizen-consumer protection. These respective policy agendas will have to meet each other in the middle somewhere,

[208] Antoinette Rouvroy & Yves Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, REINVENTING DATA PROTECTION? 45, 68-69 (Serge Gutwirth et al., 2009), http://link.springer.com/10.1007/978-1-4020-9498-9; Serge Gutwirth, PRIVACY AND THE INFORMATION AGE 86 (Raf Casert trans., Rowman & Littlefield Publishers, 2002).

[209] Benohr, *supra* note 113, at 59–60.

[210] *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a European Consumer Agenda—Boosting Confidence and Growth*, COM (2012) 225 final (May 22, 2012), http://ec.europa.eu/transparency/regdoc/rep/1/2012/EN/1-2012-225-EN-F1-1.Pdf.

[211] *REFIT Fitness Check of Consumer Law*, EUR. COMMISSION (December 2015), http://ec.europa.eu/smart-regulation/roadmaps/docs/2016_just_023_evaluation_consumer_law_en.pdf.

[212] Robert & Smit, *supra* note 151, at 18–19.

المنارة للاستشارات
www.

and it may be left to the Court of Justice to sort out the conceptual mess. The analysis in this Article has shown that in the context of pre-formulated declarations of consent, such a collaborative role can be carved out with respect to the relevant frameworks and the intent of the three respective policy agendas. A more concurrent substantive application of protections with delineated but complementary enforcement of the respective frameworks is needed to empower citizen-consumers.

Cite this article: Clifford D, Graef I, and Valcke P (2019). Pre-formulated Declarations of Data Subject Consent—Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections. *German Law Journal* **20**, 679–721. https://doi.org/10.1017/glj.2019.56

المنارة للاستشارات

www.

© 2019 This article is published under (http://creativecommons.org/licenses/by-nc-nd/3.0/)(the "License"). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License.

المنارة للاستشارات

www.