Taking proportionality seriously. The use of contextual integrity for a more informed and transparent analysis in EU data protection law

Abstract (156 words):

Difficulties abound as to where the boundary between legitimate and illegitimate processing of personal data must be set. The open-ended wording of the EU Data Protection Directive (DPD) 95/46 leaves space for diverse interpretations. The European Court of Justice finds it difficult to establish methodically the contextual data flows associated with individuals' rights and the processing, with cascading consequences for the proportionality analysis, thus echoing the wider debate on proportionality. Taking stock of the criticisms of the ECJ's decisions and of the changes introduced by the General Data Protection Regulation, this paper proposes to use contextual integrity, a framework of analysis developed by Helen Nissembaum, largely implicit in EU data protection law, to provide a systematic method of interpretation that ensures more consistency in current EU legal practice. It recommends adopting a new formal three-tier structure, so that all factors necessary to the discussion on proportionality are fully and systematically identified and proportionality is taken seriously.

Key words: data protection, privacy, context, contextual integrity, proportionality

I - Introduction

Processing personal data entails seeking to strike a highly delicate balance between two competing objectives: on the one hand enabling the free flow of data at the heart of technological innovations, and on the other hand safeguarding individuals' rights and freedoms, most notably their rights to privacy and data protection. Recognising this tension in its Article 1, the EU Data Protection Directive (DPD), the main legal instrument of the current European data protection framework, provides key principles for determining which personal data processing practices are or are not acceptable. Nevertheless, the DPD's broad wording means its 'interpretation [notably of its proportionality requirement] is no easy task' [1]. Taking stock of the diverse interpretations that have emerged and the changes introduced by the General Data Protection Regulation (GDPR), this paper proposes to use contextual integrity (CI), a framework of analysis developed by Helen Nissembaum, largely implicit in EU data protection law, to provide a systematic method of interpretation that promotes a more informed and transparent proportionality analysis and ensures more consistency in current EU legal practice.[2]

To date, as evidenced in recent decisions of the Court of Justice of the European Union (ECJ), processing practices adopted by some businesses and part of the public sector rest on an interpretation which facilitates extensive data harvesting, profiling and monitoring of individuals. In reaction, citizens are pushing, with the ECJ's blessing, for a different boundary between legitimate and illegitimate data flows which better protects their rights and reflects a more nuanced balance between rights and

[1] L. Bygrave, *Data privacy law: An international perspective* (OUP, 2014) at 56.
[2] H. Nissenbaum, 'Protecting Privacy in the Information Age: the Problem of Privacy in Public', (1998) 17 *Law and Philosophy* 559

interests under the DPD. [3] However, despite the ECJ's response being well received, strong criticisms of the ECJ's case law endure, fuelling uncertainties about where this boundary should be set. [4] Scholars criticise the ECJ for shortcomings in identifying, at a preliminary stage, the various elements that need to be balanced when assessing the proportionality of data processing interference with individuals' rights with the legitimate aims pursued by data controllers. The ECJ has not examined in sufficient detail data controllers' legitimate interests in processing data or the data subjects' rights that such processing infringes. Consequently, the ECJ's weighting and discussion of these elements at the subsequent proportionality stage has been presented as inadequate and even as 'unworkable formulae'[5], a criticism echoing the wider debate on proportionality in constitutional adjudication.[6]

This leaves the various actors who process personal data in a difficult position when having to determine effectively where the boundary between legitimate and illegitimate data flows lies. [7] Indeed, the General Data Protection Regulation (GDPR), which will replace the DPD by 25 May 2018, notes the need to enhance 'legal and practical certainty' for all stakeholders in interpreting data protection

[3] Case 131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* [2014] 3 C.M.L.R. 50; linked to third-country transfers, Case 362/14 *Maximillian Schrems v Data Protection Commissioner*, [2016] 2 C.M.L.R. 2; and the territorial application of the Directive 95/46, Case 230/14, *Weltimmo s.r.o v Nemzeti Adatvédelmi és Információszabadság Hatóság*, OJ C 381, 16/11/2015, 6; Joined Cases 203/15 and 698/15, *Tele2 Sverige AB and Watson*, 21 December 2016

[4] Ch. Tranberg, 'Proportionality and data protection in the case law of the European Court of Justice', (2011) 1 *International Data Privacy Law* 239; E. Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos', (2014) 14 *Human Rights Law Review* 761; D. Erdos, 'From the Scylla of Restriction to the Charybdis of Licence? Exploring the scope of the 'special purposes' freedom of expression shield in European data protection', (2015) 52 Common Market Law Review 119; Ch. Kuner, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges', *in* B. Hess and Ch. Mariottini (eds.), *Protecting Privacy in Private International and Procedural Law and by Data Protection* (Routledge, 2015) at 19; O. Lynskey, 'Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order', (2014) 63 ICLQ 569; O. Lynskey, 'Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez', (2015) 78 *The Modern Law Review* 522; to a lesser extent, D. Sancho-Villa, 'Developing Search Engine Law: It Is Not Just about the Right to Be Forgotten', (2015) 42 *Legal Issues of Economic Integration* 357, 373; S. Peers and S. Prechal, 'Article 52 – Scope and Interpretation of Rights and Principles' in Peers, Hervey, Kenner, and Ward (eds), *The EU Charter of Fundamental Rights. A Commentary*, (Hart Pub, 2014), at 1455, para. 52.84 -54.86.

[5] F. Fontanelli, 'The mythology of proportionality in judgments of the Court of Justice of the European Union on internet and fundamental rights.' 36 *Oxford Journal of Legal Studies* (2016), 630-660, at 640.

[6] See for e.g., S. Tsakyrakis, 'Proportionality: An assault on human rights?' (2009) 7(3) *International Journal of Constitutional Law* 468; M. Khosla,'Proportionality: An assault on human rights?: A reply.' (2010) 8(2) *International Journal of Constitutional Law* 298; S. Tsakyrakis, 'Proportionality: An assault on human rights?: A rejoinder to Madhav Khosla' (2010) 8(2) *International Journal of Constitutional Law* 307; K. Lenaerts, and J. Gutiérrez-Fons, 'The constitutional allocation of powers and general principles of EU law' (2010) 47 *Common Market Law Review* 1629, at 1652-1653; K. Möller, 'Proportionality: Challenging the critics' (2012) 10 *International journal of constitutional law* 709; R. Alexy, 'On balancing and subsumption. A structural comparison.' (2003) 16(4) *Ratio Juris* 433, 437-439; R. Alexy, 'Formal principles: Some replies to critics.' (2014) 12(3) *International Journal of Constitutional Law* 511. See also L. Niglia, 'Eclipse of the Constitution {Europe Nouveau Siècle}' (2016) 22(2) *European Law* Journal 132, 143-144, 154.

[7] F. Fontanelli, n 5 supra, 645; O. Lynskey, 2015, n 3 supra, 531-532; E. Frantziou, n 4 supra, 770; M. Oswald, 'Seek, and Ye Shall Not Necessarily Find: The Google Spain Decision, the Surveillant on the Street and Privacy Vigilantism' in K O'Hara, MHC Nguyen and P Haynes (eds), *Digital Enlightenment Yearbook 2014: Social Networks and Social Machines, Surveillance and Empowerment* (2014) at 99.

rules, given the importance of creating the trust that will allow the digital economy to develop', [8] a trust currently eroded as European Union citizens feel they have hardly any control over their data. [9]

This paper explores how the boundary between legitimate and illegitimate processing practices can be established more consistently and transparently in the DPD as interpreted by the ECJ, and in the GDPR, by using contextual integrity to facilitate the methodical organisation of the proportionality analysis.

Highly influential in the US despite some criticisms, CI is also intended to be 'a justificatory framework for all people and all societies'[10] - including in the EU - that 'can serve as a foundation for law and regulation by providing a standard against which legislation (existing or proposed) and detailed rules are tested'[11] when determining the boundaries between legitimate and illegitimate data flows. The central tenet of CI is that a satisfying discussion of the contested processing depends not simply on establishing the rights which will be discussed at the proportionality stage but also on identifying, beforehand, the context and all data flows which these rights generate. To date, only one study asserted that EU data protection law integrates CI and would not be improved by reference to CI[12]; but no systematic study has demonstrated whether CI, in its two components of context and informational flows, is integrated into current and future EU data protection law, and what benefits CI could bring. [13]

This paper proposes doing precisely this. It will start with a presentation of the challenges in EU data protection law, notably the criticisms addressed at the ECJ's proportionality assessment, and how these criticisms fit within the wider debate on proportionality. These challenges will be subsequently appraised in light of the contextual integrity framework, to be further explained. This paper will then demonstrate that each of the two fundamental CI concepts of context and informational flows related to the processing practices that interfere with data subjects' rights implicitly underpin the legal analysis in the DPD, including as interpreted by the ECJ, and feature expressly in various provisions of the GDPR.

---

[8] Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) O.J. 2106, L119/1, Recital 7.

[9] *OECD Digital Economy Outlook 2015*, (OECD Publishing, 2015), at 62-64; Eurobarometer 431, Data Protection, Summary, June 2015, available at http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf (accessed 04 February 2017) and for the full report, http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf (accessed 04 February 2017); for the US, J. Turow, M. Hennessy, and N. Draper, 'The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation.' *The Annenberg School for Communication, University of Pennsylvania* (2015), at https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_0.pdf (accessed 04 February 2017); H. Hijmans & H. Kranenborg, 'Data Protection Anno 2014: How to Restore Trust? An Introduction', in H. Hijmans and H. Kranenborg (eds), *Data Protection Anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004–2014)*, (Intersentia, 2014), 3, at 6, 14-15. See also F. Grodzinsky and H. Tavani. 'Privacy in the cloud: applying Nissenbaum's theory of contextual integrity.' (2011) *ACM SIGCAS Computers and Society* 41(1), 38, at 39-40; H. Nissenbaum, 'A Contextual Approach to Privacy Online', in J. Bus, M. Crompton, M. Hildebrandt, and G. Metakides (eds) *Digital enlightenment yearbook 2012*, (IOS Press, 2012), 219, at 221

[10] H. Nissenbaum, *Privacy in context: Technology, policy, and the integrity of social life*, (Stanford University Press, 2009) at 16

[11] Id, at 236

[12] K. Irion and G. Luchetta, 'Online personal data processing and EU data protection reform' (8 April 2013) *CEPS Task Force. Report of the CEPS Digital Forum*. Centre for European Policy Studies 2013, at 57, available at SSRN: http://ssrn.com/abstract=2275267

[13] K. Irion and G. Luchetta do not demonstrate how EU law integrates CI, n12 supra, at 57. Despite a page on Nissenbaum's framework, Bunn declined to apply CI to her analysis of the *Google Spain* decision. A. Bunn, 'The curious case of the right to be forgotten.' (2015) 31 *Computer Law & Security Review* 336.

However, these elements are not integrated into a well-defined framework that can serve as a robust foundation for a proportionality analysis. This paper submits that, in spite of the criticisms directed at CI, [14] CI helps with formalising and giving substance to current legal analysis, and thus guides the proportionality analysis through recognizable elements which can be evaluated and re-evaluated in later decisions, bringing increased coherence and predictability to the interpretation of the DPD and GDPR. Hence, the recommendation that all stakeholders adopt a new three-tier structure, with a formal analysis of context in addition to the existing examination of all contextual data flows so that all factors necessary to the discussion on proportionality are fully and systematically identified.

II – The challenges in EU data protection law

As a directive, the DPD does not aim to set detailed guidelines. Whilst its broad wording offers enough flexibility for the principles to apply across a wide range of processing situations, it also leaves space for potential differences and difficulties in interpretation. This section will thus sketch the essential features of the analysis in the DPD as a general background to the criticisms directed at the ECJ's interpretation of the DPD, present these criticisms replacing them within the wider debate on proportionality, and briefly outline the advances made by the GDPR.

A – The gaps in the DPD

The DPD establishes a series of 'checks and balances'[15] that guides data controllers into the determination of 'fair and lawful' data processing practices (Article 6(1)(a) DPD). The key principles are found in Articles 6 and 7 DPD, with Article 8 DPD providing a different set of limitations from that of Article 7 DPD when the personal data are sensitive, i.e. pertaining to race, ethnicity, health, religious or philosophical beliefs, political opinions and trade union membership. [16] These articles clearly establish a two-steps analysis: a preliminary step to identify the legitimate purposes justifying the processing, and a subsequent assessment of the processing's proportionality with the purposes identified. Furthermore, the general objective of the DPD as stated in Article 1 points towards an additional step where data subjects' rights which the processing may interfere with have to be identified prior to the proportionality assessment. We will outline these three steps while pointing to the potential issues causing authoritative interpretation of the ECJ to be needed.

In accordance with Article 6(1)(b) DPD, and on the basis that the data processed are personal data, the analysis begins by determining the 'specified, explicit and legitimate purposes', i.e. the immediate

[14] M. Birnhack, 'Review: A Quest For A Theory Of Privacy: Context and Control' (2011) 51 *Jurimetrics* 447; to a lesser extent, S. Dawes, 'Privacy and the public/private dichotomy' (2011) 107(1) *Thesis Eleven* 115.
[15] H. Kranenborg, 'Article 8–Protection of Personal Data' in S. Peers, T. Hervey, J. Kenner and A. Ward (eds), *The EU Charter of Fundamental* Rights. *A Commentary,* (Hart Pub 2014) at 223, para 8.26.
[16] Article 29 WP presents Article 8 DPD as the 'lex specialis', *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP 217, 9 April 2014, at 14

reasons for which personal data is collected. These can include, for example, to facilitate registration on a website, to enable payment or to send a catalogue as part of a marketing strategy. For these original purposes to be legitimate, the processing must be based on one of the legal grounds provided for in Article 7 DPD, for example, with the data subject's consent (Article 7(a) DPD), for the performance of a contract (Article 7(b) DPD) or 'for the purposes of the legitimate interests of the controller or third party' (Article 7(f) DPD).

This assessment of a purpose's legitimacy is complex. How to choose the correct legal ground listed in Article 7 DPD depends on the interpretation of each ground, taken individually and in relation to each other. In practice, Article 7(f) DPD has proved one of the most controversial provisions. Relying extensively on this ground rather than on the others listed in Article 7 DPD, data controllers have interpreted Article 7(f) DPD's undefined expression 'for the purposes of the legitimate interests of the controller or third party' so broadly that they tend to justify any processing of personal data, including that which arguably violates the data subjects' rights. [17] This problematic assessment of Article 7(f) DPD, and more generally of the legitimacy of the purposes, has far reaching consequences. The identification of the correct legal ground is essential 'to establish the boundaries within which personal data collected for a given purpose may be processed and may be put to further use.'[18] Further processing is only permitted if it is compatible with the legitimate purpose established for the collection of data. Choosing the wrong legal ground at the time of collection cannot be remedied later on to validate further uses of data retrospectively. [19]

In its guidance on the interpretation of the legitimacy requirement, the Article 29 Data Protection Working Party (Article 29 WP) advisory body recommends taking into account the context in which the processing operates and 'which determines the reasonable expectations of [the?] data subject' regarding the use and further use of data. [20] It re-emphasises the role of context in choosing which legal ground of Article 7 DPD may justify the processing and as a factor in adequately identifying the legitimate interests of the data controller or third parties of Article 7(f) DPD. [21] With regard to further processing, Article 29 WP again presents context and the data subjects' expectations of further use as two key factors for determining whether further processing is or is not compatible with the original purposes specified at collection.[22] This concept of the expectations of data subjects recalls the concept of 'reasonable expectations of privacy' developed by the European Court of Human Rights when interpreting Article 8 of the European Convention for Human Rights (ECHR), which guarantees the right to privacy.[23] However, the DPD mentions none of these factors; whether they ought to be systematically included in the analysis of the purpose of processing is unclear. It is also unclear what

[17] Id at 3
[18] *Opinion 03/2013 on purpose limitation,* WP 203, 2 April 2013, at 4
[19] WP 203, n 17 supra, at 36
[20] Id at 13, 19-20
[21] *Opinion 15/2011 on the definition of consent*, WP 187, 13 July 2001, at 2, 6-8, 12-14; WP 217, n 15 supra, at 13
[22] WP 203, n 18 supra, at 24; see H. Kranenborg, n 15 supra, para 8.103.
[23] Notably, ECtHR, *Lüdi v. Switzerland*, App. No 12433/86, A-238, judgment of 15 June 1992; ECtHR, *Halford v. The United Kingdom* Appl. No. 20605/92, 1997-III, judgment of 25 June 1997; ECtHR, *PG and JH v United Kingdom*, App No 44787/98, judgment of 25 September 2001; ECtHR, *Von Hannover v Germany,* App. No *59320/00*, judgment of 24 June 2004; ECtHR, *Re v* The *United Kingdom,* Appl. No 62498/11, judgment of 27 October 2015; ECtHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland*, App. No 931/13, judgment of 27 June 2017.

context comprises, since Article 29 WP does not provide a definition. The ECJ's interpretation of Articles 6 and 7 DPD will thus be crucial to understanding the purpose requirement and legal grounds of Article 7 DPD.

This analysis under Articles 6 & 7 DPD of the legitimate purpose, and subsequently of the proportionality of processing, must be conducted with regard to the DPD's two-fold objective as stated in Article 1: to 'protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data' and to facilitate the flows of data stemming from the processing. Thus, when processing interferes with an individual's rights, the analysis becomes a three-step process. In addition to identifying the processing's legitimate purpose, the data subjects' right(s) which are being interfered with should be determined prior to their weighting.

Only Article 7(f) DPD expressly refers to this identification of the rights interfered with, stating that processing for the purposes of legitimate interests pursued by the controller or third parties may not be possible 'where such interests are overridden by the *interests [or] fundamental rights and freedoms* of the data subject which require *protection under Article 1(1)*' (our emphasis). Although Article 9 DPD identifies the right interfered with as the right to privacy, which must be balanced against freedom of expression, the rest of the DPD is silent on this second step of the analysis. The ECJ will thus have to confirm that, in light of Article 1 DPD, the analysis includes the finding of interference with data subjects' rights.

The rights that processing may interfere with may be the data subjects' right to not be discriminated against[24] or their freedom of expression.[25] However, in most cases, they will be the data subjects' rights to privacy and data protection, as protected by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (Charter). The right to data protection emerged from, and is thus closely related to, the right to private life under Article 8 ECHR. [26] Yet, the right to data protection is not identical to the right to privacy, despite the two rights often being referred to together. The right to data protection is an autonomous fundamental right recognised in Article 8 of the Charter, distinct from Article 7 of the Charter protecting the right to privacy. [27] Its elements are based on the DPD, with the first one stating the conditions of processing data by reference to the DPD's core principles in Articles 6 and 7 DPD. [28]

[24] Case 524/06, *Huber v Germany*, [2008] ECR I-9705; H. Kranenborg, n 14, paras. 8.43-8.44, 8.121; L. Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International, 2002), at 125-159.
[25] Case 70/10, *Scarlet Extended v Société Belge des Auteurs, Compositeurs et Editeurs SCRL* (SABAM), [2011] ECR I-11959; Case 461/10, *Bonnier Audio AB v Perfect Communication Sweden AB*, [2012] 2 CMLR. 42; Case 275/06 *Productores de Música de Espana (Promusicae) v Telefónica de Espana SAU,* [2008] ECR I-271.
[26] On the sources of Article 8 Charter, H. Kranenborg, n 15 supra, paras. 8.50-8.68
[27] J. Kokott and Ch. Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', in Hijmans and Kranenborg (eds), n 9 supra, at 83-95; O. Lynskey, 'Deconstructing data protection…', n 4 supra; Article 29 WP, 'The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data', WP 168, 01 December 2009, at 5.
[28] Explanations relating to the Charter of Fundamental Rights of the European Union, O.J., C 303/17, at 21. The second element is the data subjects' rights to access and to the rectification of the data processed; and the third, the requirement that 'compliance with these rules' is under 'the control of an independent authority'. See also Case 31/12, *Google Spain*, para 69.

Any limitations to these rights guaranteed by the Charter will have to be analysed in light of Article 52(1) of the Charter, which states that limitations must respect the essence of rights and be provided by law, and that, '[s]ubject to the principle of proportionality, [they] 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.' As the ECHR also guarantees the right to privacy and freedom of expression, restrictions on these rights will have to comply with ECHR case law. The articulation between the ECHR and the Charter is set out in Article 52(3) of the Charter, which requires 'the meaning and scope of those rights [in the Charter to] be the same' as those in the ECHR, although 'Union law [may] provi[de] more extensive protection'. However, how the analysis in the Charter and the ECHR fits with that of Articles 6 and 7 DPD is not clearly set out in the texts.

Regarding the first step of the analysis, for Article 29 WP, both the purposes and the legal grounds of Article 7 DPD are concepts 'first used as a requirement in the context of derogations to privacy rights'. They 'subsequently developed into a full principle in data protection law', beyond the right to privacy, but remain related to the concept of 'legitimate aim' in Article 8 ECHR as interpreted by the ECtHR. [29] They also interrelate with the legitimate objectives listed in Article 52 of the Charter: the 'objectives of general interest recognised by the Union' and 'the need to protect the rights and freedoms of others'.

Consequently, the question is whether the identification of legitimate purposes in the DPD extends to identifying 'the general interest' and/or 'the rights and freedoms of others' that may form or be connected to the legitimate objective pursued by the data controller when processing data. Some DPD provisions expressly call for this identification.[30] Other provisions are more implicit but leave little doubt that the rights and/or interests in the processing must be identified.[31] Other provisions, like Article 7(f) DPD, are ambiguous. Article 7(f) DPD refers solely to the data controllers' and third parties' 'legitimate interests', whereas for the data subjects, it asks us to identify either their 'interests' or their 'fundamental rights'. Thus, 'legitimate interests' seems a narrow concept. However, for Article 29 WP, the balancing in Article 7(f) DPD between the legitimate interests of the data controller and the data subjects' rights will differ according to whether the 'legitimate interests' are rather 'trivial' or, on the contrary, 'compelling and beneficial to society at large, such as the interest of the press to publish information about government corruption'. [32] Accordingly, Article 29 WP recommends conducting, prior to the balancing, a detailed analysis of the legitimate interests in Article 7(f) DPD, not only by identifying the context of the processing, as seen earlier, but also by finding out whether or not the data controller exercises a fundamental right, pursues a public interest or serves the interest of a wider community. [33] Article 29 WP favours an interpretation of Article 7(f) DPD that uncovers the various

[29] WP 203, n 18 supra, p7; WP 217, n 16 supra, at 6, 17.
[30] Directive 95/46, Art. 8(2)(b), 9 and 13(1)(g).
[31] Directive 95/46, Art. 8, with Recital 33.
[32] WP 217, n 16 supra, at 24, 34.
[33] WP 217, n 16 supra, at 3, 34-36.

factors –context, rights and collective goods- that may gravitate around the data controller's and/or third parties' legitimate interests. Yet, Article 7(f) DPD does not mention them. The ECJ will have to articulate what the identification of the 'legitimate interests' entails.

Regarding the proportionality assessment in the DPD and its articulation with the Charter and the ECHR, the word 'proportionality' does not appear in the DPD. [34] The data must be 'adequate, relevant and not excessive' with regard to the purpose specified (Article 6(1)(c) DPD), and must be processed for 'no longer than necessary for the purposes' which justify collection or further use of data (Article 6(1)(e) DPD). [35] The processing must also be 'necessary' to the legal ground identified in light of Article 7 DPD but 'necessary' is not defined. However, the principle of proportionality is a long-standing principle of EU law outside the field of data protection law. [36] It is also central to the protection of fundamental rights in the Charter and in the ECHR. Thus, these various proportionality tests and what they entail should interpolate with the proportionality requirement in the DPD, although it remains for the ECJ to articulate how they do so and whether the factors necessary to the analyses of proportionality overlap.

To summarize, the structure of an analysis is likely to include two preliminary steps - identifying the legitimate objective pursued by the data controller when processing data, and finding out whether the processing interferes with data subjects' rights – before assessing the proportionality of the processing. The ECJ's interpretation of the DPD will be crucial to understand how the proportionality requirement in the DPD should be interpreted, in particular: whether the correct identification of legitimate purposes depends on establishing the context of the processing and the related expectations of data subjects as to the uses and further uses of data; whether Article 7(f) DPD – or other grounds of processing- requires more than just identifying 'the legitimate interests of the data controllers or third parties' and according to which criteria: context, data controller's or third parties' right(s) and broader interests of the wider community.

B – The ECJ's interpretation of the DPD and its criticisms in light of the wider concerns on proportionality in constitutional adjudication

The ECJ confirmed that 'the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must

[34] L. Bygrave, n 1 supra, at 148.
[35] Data must also be accurate and when necessary up to date (Article 6(1)(d) Directive 95/46). There are a number of derogations to these principles, but given their complexity and the objective of this section, the derogations will not be examined here.
[36] L. Bygrave, n 1 supra, p. 148; Ch. Tranberg, n 4 supra, at 240; see further, P. Craig and G. De Búrca, *EU Law* (OUP, 2015) at 526-33; T.I. Harbo, 'The Function of the Proportionality Principle in EU Law', (2010) 16 *European Law Journal* 158, 165.

necessarily be interpreted in the light of fundamental rights', [37] a situation which is 'characteristic of the interpretation of the Data Protection Directive'.[38] The analysis thus has two steps prior to the proportionality assessment: the identification of a legitimate objective, and finding interference and assessing its seriousness. Furthermore, the ECJ specifies that a breach of Article 8 ECHR leads to a breach of the necessity criterion of the DPD. [39] Although the ECJ does not consistently refer to Article 52(1) of the Charter in its decisions, [40] it has also affirmed that interference with data subjects' rights 'recognised by Articles 7 and 8 of the Charter [must be] justified having regard to Article 52(1) of the Charter'. [41] The ECJ thus applies the traditional three-prong test of proportionality: suitability (is the measure suitable, appropriate or relevant to the legitimate objective pursued?), necessity (is the measure required to fulfil the objective pursued and is it the least restrictive?), which often the ECJ merges with the third prong, [42] proportionality *stricto sensu*, which consists of a weighting of interests where the interference with fundamental rights is assessed against the importance of the objective pursued to determine whether or not there is an undue burden on the individual. [43]

With regards to proportionality *stricto sensu*, it was initially felt that, in a number of cases, [44] the ECJ did not provide sufficient guidelines to the national courts on how to strike a balance between conflicting fundamental rights. [45] With subsequent cases, [46] many of these early criticisms proved unfounded.[47] Nevertheless, the ECJ remains criticised for the poor quality of its balancing, due to its failure to first establish in greater details the two main aspects of its analysis: the processing's legitimate objective(s), and the interference with the data subjects' rights. A review of these criticisms will be followed by a presentation of the wider context, i.e. the debate on proportionality.

---

[37] Case 131/12, para 68. The Court cited the Joined Cases 465/00, 138/01 and 139/01, *Rechnungshof v Österreichischer Rundfunk*, [2003] ECR I-4989; Case 212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, OJ C 46, 09/02/2015 at 6, para 29

[38] Case 73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy* (*Satamedia*), [2008] ECR I-9831, Opinion of AG Kokott, EU:C:2008:266, para 44

[39] Case 465/00, *Rechnunghof*, para 91

[40] H. Kranenborg, n 15 supra, para. 8.163-8.164; S. Peers and S. Prechal, n 4 supra, paras. 52.53-52.56, 52.61

[41] Joined Cases 92/09 & C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, [2010] ECR I-11063, para 64; Case 291/12 *Michael Schwarz v Stadt Bochum*, EU:C:2013:670, para 33

[42] Case 465/00, *Rechnunghof*, para 76, 82-83; Case 73/07, *Satamedia*, para 56; Joined Cases 92/09 & C-93/09, *Schecke* para 74; Case 212/13, *Rynes*, para 28; Case 362/14 *Schrems*, para 92

[43] R. Alexy, *A Theory of Constitutional Rights* (Trans. Julian Rivers) (Oxford University Press, 2002). (1st. ed. in German 1985), 102; P. Craig and G. de Burca, n 36 supra, at 526-33; T. Tridimas, *The General Principles of EU Law* (Oxford University Press, 3rd ed, at 139; T.I. Harbo, n 36 supra, 165; M. Cohen-Eliya, Moshe and I. Porat, 'American balancing and German proportionality: The historical origins.' (2010) 8(2) *International Journal of Constitutional Law* 263.

[44] Case 465/00, *Rechnunghof*, para 88; Case 101/01, *Bodil Lindqvist*, [2003] ECR I-12971; Case 73/07, *Satamedia*; Case 275/06 *Promusicae*.

[45] P. Oliver, 'The protection of privacy in the economic sphere before the European Court of Justice.', (2009) 46 *Common Market Law Review* 1443; M. Tzanou, 'Balancing Fundamental Rights: United in diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection.', (2010) 6 *Croatian Yearbook of European Law and Policy* 53; F. Coudert and E. Werkers, 'In the aftermath of the Promusicae case: how to strike the balance?', (2010) 18 *International Journal of Law and Information Technology* 50, 51. Contra X. Groussot, 'Rock the KaZaA: Another Clash of Fundamental Rights', (2008) 45 *Common Market Law Review* 1745, 1761; H. Kranenborg, n 15 supra, para 8.42; S. Peers and S. Prechal, n 4 supra, paras. 52.55, 52.64.

[46] Case 70/10, *Scarlet Extended*; Case 360/10, *SABAM v Netlog*.

[47] L. Bygrave, n 1 supra, at 149; D. Erdos, n 4 supra, 130-132; F. Ferretti, 'Data protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights?' (2014) 51 *Common Market Law Review* 843, 860-861; contra F Fontanelli, n 5 supra, 651-652.

The first set of criticisms concerns the ECJ's perceived restrictive approach to the determination of the data controller's legitimate objective in light of Article 52(1) of the Charter and/or with regard to the wording of Article 7(f) DPD. For critics, if the ECJ had identified the rights which exercise the processing may facilitate or reflect, its balancing at the proportionality stage would have been more complete and precise. Three cases illustrate the matter.

In *Schecke*, the ECJ had to interpret Regulation 45/2001, which transposed the DPD for the EU institutions. The question was whether the objective of transparency could justify the EU Commission and EU Council requiring the publication of the names of individuals who received EU subsidies. Assessing the question in light of Article 52(1) of the Charter, the ECJ considered that the objective of transparency pursued by the EU institutions constituted an 'objective of general interest recognised by the Union'. However, it did not enquire, as Article 52(1) of the Charter suggests, as to whether the legitimate objective could also facilitate the protection of the rights and freedoms of others, here the exercise by EU citizens of their right to access European Parliament, Council and Commission documents under Article 42 of the Charter. By not extending its analysis beyond the 'general interest', the ECJ might have sought to exercise judicial restraint,[48] but some have argued that the ECJ should have identified the rights that needed to be protected rather than just the data controller's 'interest', with the consequence that the balancing test would have been different. [49]

This issue extends to the interpretation of Article 7(f) DPD. In *Asnef*, a credit bureau and a marketing company which wished to process data as part of their business contested the blanket ban that Spanish authorities established on the processing of all private data. [50] Although the ECJ initially cited Article 52(1) of the Charter, it focused solely on interpreting the DPD. It accepted that the ban violated Article 7(f) DPD, and thus implicitly recognised the companies' legitimate interests in processing data. However, it did not enquire as to whether the legitimate interests may reflect the exercise of the companies' right to conduct business as guaranteed by Article 16 of the Charter. [51] The ECJ was faithful to the wording of Article 7(f) DPD, but there were concerns about the subsequent balancing, since the interests for processing could 'be interpreted as prevailing over established rights' and that the data subjects' right to privacy would then be impoverished. [52] It is indeed a familiar

[48] M. Bobek, 'Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifer*t, Judgement of the Court of Justice (Grand Chamber) of 9 November 2010 NYR.' (2011) 48 *Common Market Law Review* 2005, at 2015.
[49] S. Peers and S. Perchal, n 4 supra, para 52.51; A-S. Lind and M. Strand, 'A New Proportionality Test for Fundamental Rights?: The Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen. Report', in Swedish Institute for European Policy Studies, (2011) *European Policy Analysis* 7 http://www.sieps.se/sites/default/files/2011_7epa.pdf (accessed 04 February 2017); for the link between transparency and Article 42 Charter, see P. Leino, 'Just a little sunshine in the rain: the 2010 case law of the European Court of Justice on access to documents.' (2011) 48 *Common Market Law Review* 1215, at 1217.
[50] Joined Cases 468/10 and 469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado*, [2011] ECR I-12181.
[51] S. Peers and S. Prechal, n 4 supra, paras. 52.61, 52.72
[52] F. Ferretti, n 47 supra, 865-866

criticism in human rights law, beyond the field of data protection law, that balancing interests against fundamental rights, instead of rights against rights, may lower the protection due to fundamental rights.[53] Consequently, it was submitted that the interests should prevail only when they are 'upheld by the law' and correspond to a data controller or a third party exercising a fundamental right.[54]

With *Google Spain*, this danger of interests overriding rights seems to have been averted. The ECJ had to decide whether or not a data subject could request that search engine Google stop processing some personal data and thus delist a link to personal information appearing in search results. Google justified its processing on the basis of its legitimate interests and of those of third parties as per Article 7(f) DPD. The ECJ identified these interests, referred to as 'economic interests',[55] for Google as data controller, and for third parties as 'the legitimate interest of internet users potentially interested in having access to that information'. [56] The ECJ also named data subjects' rights to privacy and data protection. Following the wording of Article 7(f) DPD, with no reference to Article 52(1) of the Charter, it then declared that data subjects' rights 'override as a rule' the legitimate interests of a data controller and internet users.[57] The apparent effect of the *Google Spain* decision is to strengthen data subjects' position rather than weakening it, thus putting an end to the concerns about the balancing outcome expressed after *Asnef*.

Nevertheless, the decision has attracted strong criticisms, for the same reasons as before: the ECJ's failure to establish the fundamental rights which exercise Google's processing facilitates, with the consequence that the ECJ did not discuss the contextually relevant positions of these rights. The ECJ did not follow Article 29 WP's interpretation of Article 7(f) DPD about the data controller's legitimate interests. It did not identify Google's right to conduct a business pursuant to Article 16 of the Charter, whereas its Advocate General did;[58] and thus did not discuss which weight to attach to this right, or how Google's business would be impacted by the measure the ECJ imposed on Google.[59] It did not identify either 'the legitimate interest of internet users […] in having access to that information' as their freedom of information and expression protected by Article 11 of the Charter and Article 10 of the ECHR. Consequently, it did not discuss the role of private actors such as Google have in enabling the public to exercise this fundamental right, and how as a collective good, this right could be weighted against an individual's right to privacy. Thus, the ECJ's balancing was presented as one-sided, biased towards strong protection of data subjects' rights that peremptorily disregarded the freedom of

[53] S. Tsakyrakis, n 6 supra, 470-472; F. Fontanelli, n 5 supra, 631-632; but, M. Khosla n 6 supra, 300-305; K. Möller, n 6 supra, 717-721; K. Lenaerts, and J. Gutiérrez-Fons, n 6 supra, 1652-1653.

[54] F. Ferretti, n 47 supra, 866.

[55] Case 131/12, *Google Spain*, paras. 56, 81, 97, 99; contrast with Case 70/10, *Scarlet Extended*; Case 360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, [2012] CMLR 18; Case 461/10, *Bonnier*, where ISPs are recognized expressly a right to conduct business.

[56] Case 131/12, *Google Spain*, para 81.

[57] Id para 97. In the English version, Article 7(f) DPD uses the verb 'to override', but in French, refers to 'to prevail' (prevaloir). Although respectful of the DPD's wording, the ECJ's choice of terms may not help appeasing those concern about freedom of expression as the English verb suggests an additional imperative absent in the other languages. To override would be translated in French by 'supplanter' (to supplant) or even 'passer outre', the latter meaning 'to carry on regardless of'. All versions of Google Spain though keep the expression 'as a rule', absent from the text of the Directive.

[58] Advocate General, Opinion, EU:C:2013:424, para 95; for the ECJ, see also Case 70/10, *Scarlet Extended*, para 48.

[59] F. Fontanelli, n 5 supra, 644-645

expression of internet users. [60] The ECJ was said to have compromised its ability to provide effective guidance on how all the rights at stake, not just the right to privacy, shape the boundary between legitimate and illegitimate processing practices.

The second set of criticisms concerns the *Bavarian Lager* (*BL*) and *Google Spain* decisions but also raises more general questions about which factors the ECJ must identify and take into account when assessing the interference with data subjects' rights.

In *BL*, where the courts had to interpret Regulation 45/2001 which transposed the DPD, the question before the EU Courts was whether or not publishing the names of company representatives present at a meeting constituted interference with the right to privacy and, if so, whether the interference was justified.[61] Three different answers were given. For the General Court (GC), although Article 8 ECHR does not exclude 'professional or business activities' from the concept of private life, i.e. interactions 'in [a] public context', [62] there was no interference with the individuals' right to privacy because in these particular circumstances their participation in a meeting as part of their professional activities did 'not fall within the sphere of th[e] persons' private life'. [63] Consequently, the GC did not assess the proportionality of the processing measure. By contrast, on appeal, Advocate General Sharpston considered that there was potential interference with the right to privacy but that the context and the objective of transparency justified the interference and thus the disclosure. [64] The ECJ also found the processing measure to constitute interference with the data subjects' right but made no reference to context and reached a different outcome from that of its Advocate General.

If the criterion for defining interference with the right to privacy is the disclosure of personal data, as the ECJ implied in *BL*, then the GC could not have concluded that there was no interference. Yet, one critic argued that the GC had chosen the correct interpretation because the *context*, here the business activities, indicated that the individual could not *expect* to have a privacy interest in a name written in an official document but rather should expect the disclosure of this personal information.[65]

How to assess these conflicting interpretations is difficult in the absence of any reference to context and the expectations of data subjects in the DPD transposed in Regulation 45/2001. These two factors, we recall, were referred to by Article 29 WP but in relation to identifying the legitimate purposes justifying processing, not in relation to the interference with data subjects' rights. Looking at the Court's case law in data protection, the ECJ tends to refer to 'all the circumstances' [66] of a case in its reasoning but without more detail concerning whether this is a reference to context and/or to data

[60] O. Lynskey, 'Control over Personal Data in a Digital Age', n 4 supra, 531; Ch. Kuner, n 4 supra, 30; E. Frantziou, n 4, 769-770; F. Fontanelli, n 5 supra, 644-645

[61] Regulation 45/2001 had to be interpreted in relation to Regulation 1049/2001.

[62] Case 28/08 P, *European Commission v Bavarian Lager Co. Ltd.*, [2011] CMLR 1, para 114, citing ECtHR, *Halford*, and ECtHR, *P.G. and J.H. v. United Kingdom*, Appl. No. 44787/98, judgment of 25 September 2001; see also paras. 123, 130.

[63] Case T-194/04, *Bavarian Lager v Commission of the European Communities* [2007] ECR II-4523, para 131, and paras. 125-128.

[64] Case 28/08 P, Opinion of AG Sharpston, EU:C:2009:624, para 192

[65] O. Lynskey, 'Deconstructing data protection', n 4 supra, 583; similarly, P. Leino, n 49 supra, 1239

[66] For example, Case 465/00, *Rechnungshof*, paras. 67, 76; Case 131/12, *Google Spain*, para 94.

subjects' expectations of privacy. In *Google Spain*, the ECJ emphasized the seriousness of the interference by noting a change in the large number of actors involved and the breadth of data processed, leading to a detailed picture of a person's life.[67] Implicit in this statement is that the new processing measures challenged past expectations of privacy that rested on a smaller number of actors and collected and used data points. However, the ECJ did not expand on this change and did not use the wording 'expectations of data subjects' or refer to the ECHR case law about 'reasonable expectations of privacy'. Put differently, the ECJ did not explain in detail 'the content and reach of these rights' to privacy and data protection or 'define them in light of the changed circumstances to which they apply.'[68] Coupled with the first criticism that the ECJ did not identify in sufficient details the legitimate interests of Google and of the internet users as third parties, "the reasoning of the Court [was said to be] very cavalier in treating the steps of the proportionality analysis, and in specifying the relative strength of its variables."[69]. The ECJ did not take proportionality 'seriously'.[70]

One author went even further, that the ECJ's use of proportionality in internet-related cases is a mask for policy-based decisions and that the ECJ should drop the proportionality test and adopt 'free-style judicial reasoning' in this instance.[71] It is an extreme position, but this criticism of the ECJ fits within the wider debate as to the merits of the proportionality test in constitutional law, human rights and other areas of EU law.

Alexy, who theorised the three-prongs proportionality test developed by the German Federal Supreme Court and adopted by the ECJ, argues that, with regards to proportionality *stricto sensu*, a rational decision on the weighting of interests can be reached and is encapsulated into a weighting (mathematical) formula.[72] Conversely, others, such as Habermas and Schlink, consider that balancing lacks rational standards and is thus arbitrary and subjective 'according to customary standards and hierarchies'.[73] Tsakyrakis, 'rejecting the myth of mathematical precision', describes proportionality as saying 'nothing about how various interests are to be weighted'[74]. Proportionality assumes that 'a common metric in the weighing process' exists whereas, for Tsakyrakis, fundamental rights can promote 'incommensurable values' that cannot be balanced; and if a common metric can be found, then balancing is not needed.[75]

In response, some argue that balancing remains possible because it is contextual. So long as the ECJ is guided by the particularity of the situation and carefully structures each step of its reasoning to discuss the legal, moral or political theories it engages with, the risk of arbitrariness should be

[67] Case 131/12, *Google Spain*, para 80.
[68] E. Frantziou, n 4 supra, 768.
[69] F. Fontanelli, n 5 supra, 645.
[70] E. Frantziou, n 4 supra, 768; F. Fontanelli, n 5 supra, 647
[71] F. Fontanelli, n 5 supra, 660.
[72] Notably, R. Alexy, n 43 supra; R. Alexy, n 6 supra.
[73] J. Habermas, *Between Facts and Norms* (Trans. William Rehg) (Polity, 1996), (1st. ed. in German 1992), 259; see R. Alexy, 'On balancing and subsumption. …', n 6 supra, 436; F. Fontanelli , n 5 supra, 645
[74] S. Tsakyrakis, n 6 supra, 471-472
[75] Id.

avoided.[76] In turn, Alexy explains that the weight formula does not 'replace argumentation by calculation'[77]. One still has to establish the intensity of the interference, i.e. the degree of non-satisfaction of or detriment to the first principle; then the degrees of importance, i.e. the 'importance of satisfying the competing principle'; before finally discussing "whether the importance of satisfying the latter principle justifies the detriment to or non-satisfaction of the former"[78]. Alexy also distinguishes between the abstract weight given to rights in constitutional law, whether in national constitutions, the Charter or the EU treaties, and the concrete weight that they have when they are applied in different situations. Alexy's mathematical formula attempts to capture all the different factors that a Court should identify and discuss in a given context, bearing in mind that "the more heavily an interference with a constitutional right weighs, the greater must be the certainty of its underlying premises." (epistemic factor).[79] However, as Alexy concedes to his critics, "the weight formula, indeed, does not tell us 'how the concrete weights to be inserted into the formula are identified, measured, and compared' [165]." [80]

In data protection law, it is notably these weights that are problematic to identify and balance. As Fontanelli explains for *Google Spain*, the new technologies challenge the circumstances under which the relevant rights have developed, particularly the right to privacy; it can be 'difficult to gauge factually' the harmful effects of processing.[81] Thus, whilst acknowledging that Alexy's formula "envisages 'abundant criteria to label a proposition as correct or incorrect' and provides [...] a 'structured form of inquiry'', Fontanelli argues that balancing the rights of so many different stakeholders (data controllers, data subjects, other users of the internet) is 'a devilish task' and that proportionality, ill-suited to provide a rational outcome, should be abandoned. [82]

Yet, this advocated path does not resolve the fundamental question that led to the author's criticism of proportionality: even if it abandons proportionality, what factors should a court taken into account in its reasoning so as to reach a suitable outcome that is not perceived as arbitrary? The EU institutions were certainly not convinced to abandon proportionality as a method of adjudication when they enacted the GDPR. Despite the criticisms at the ECJ's decisions, proportionality has been confirmed as a key principle in the GDPR, with some changes introduced as an attempt to provide some answers to the criticisms.

[76] J. Bengoetxea, N. MacCormick, and L. Moral Soriano, 'Integration and integrity in the legal reasoning of the European Court of Justice', in G. De Búrca and J. Weiler (eds.), *The European Court of Justice* (OUP, 2001), 44, 64-65; T. I. Harbo, n 36 supra, 182; J.S Sampaio, 'The Contextual Nature of Proportionality and Its Relation with the Intensity of Judicial Review', in L. Coutinho, M. La Torre, and S. Smith (eds), *Judicial Activism. Ius Gentium: Comparative Perspectives on Law and Justice*, vol 44 (Springer, 2015), 137.

[77] R. Alexy, 'The Absolute and the Relative Dimensions of Constitutional Rights.', (2016) 37(1) *Oxford Journal of Legal Studies* 31, 39.

[78] R. Alexy, 'On balancing and subsumption. …', n 6 supra, 437.

[79] Id. 446

[80] R. Alexy, 'Comments and Responses', in M. Klatt (ed.) *Institutionalized reason: the jurisprudence of Robert Alexy* (Oxford University Press, 2012), 319, 334

[81] F. Fontanelli, n 5 supra, 645-647, 657-658.

[82] Id. 643, 658, 660

C – The changes in the GDPR

Describing the DPD's principles as 'sound' in Recital 9, the GDPR models its own principles on the DPD, adding the principle of data security to Article 5 GDPR, current Article 6 DPD. Although Recital 4 lists rights potentially in conflict, and states that the principle of proportionality is to be used to resolve conflicts, the wording of Article 6(1)(f) GDPR is no clearer than its current equivalent of Article 7(f) DPD. It thus remains to be seen whether the ECJ will change its interpretation of the Article in light of future Recital 4 and might consider extending its analysis to the identification of the rights and collective goods which the processing may foster. In this sense, the GDPR has the potential to be as ambiguous as the DPD and to not address the criticisms regarding the ECJ's interpretation of the DPD.

Nevertheless, a number of provisions point towards some significant advances. In contrast to the DPD, the GDPR is more explicit about the factors to take into account for analysis. It refers to context and data subjects' expectations of data flows in a number of Recitals and Articles, in particular in Recital 38 pertaining to Article 6(1)(f), equivalent to the problematic Article 7(f) DPD. However, the GDPR does not define context or specify whether it is a general requirement or one specific to the Articles and Recitals where the term appears. The wider debate on the proportionality test, as seen above, suggests that context should be a systematic element of the legal analysis; the text however brings however no certainty. Interpretation is also difficult when it comes to the concept of expectations of data subjects. The Regulation seems to include all expectations, not just data subjects' expectations of privacy, yet the text does not explain the link with context, nor does it specify whether the references to data subjects' expectations are or are not limited to the two types of processing it mentions, merely further processing (Article 6(4) GDPR) and current Article 7(f) DPD, future Article 6(1)(f) GDPR.

Thus, on the one hand, the GDPR seems to provide answers to questions raised about the factors to take into account in the DPD, as well as confirming the role of proportionality. On the other hand, though, the GDPR does not indicate in detail how those factors operate, especially whether determining the expectations of data subjects is restricted to certain forms of processing or has a more general application. This paper submits that contextual integrity brings together these questions under the GDPR as well as the criticisms directed at the ECJ's interpretation of the DPD and at the ECJ's use of the proportionality test more generally, transforming the various points into a coherent framework.

III – Appraisal of the challenges in light of contextual integrity

Before analysing EU data protection law in light of CI, it is necessary to understand what CI is in terms of the hypothesis developed by Nissenbaum and the structure of the analysis that CI promotes.

Very much embedded into the US Fourth Amendment concept of 'a reasonable expectation of privacy' [83], CI has expressly inspired US academics in all disciplines[84] as well as the US Government, which established a 'respect for context' clause in its February 2012 Consumer Privacy Bill of Rights Act proposal.[85] CI focuses on articulating an 'alternative account of privacy', [86] with Nissenbaum in later years integrating rights other than privacy more expressly, such as the right to not be discriminated against. [87] Observing that 'there are no arenas of life *not* governed by *norms of information flow*'[88], Nissenbaum deduces that each social sphere, realm or context carries implicit or explicit expectations of what the appropriate data flows will be. [89] These 'expected flows of personal information modelled'[90] *within* a given context form are what Nissenbaum calls entrenched informational norms because they have come to be intrinsically associated with the context and have grown to be our point of reference regarding what we understand as a processing of personal data proportionate to data subjects' rights, notably their right to privacy.

When the flow of information that a processing measure creates matches these expectations contextual integrity is preserved. When the flow challenges these expectations the change points to a violation of contextual integrity, i.e. of our understanding of privacy as established so far. [91] This presumption that entrenched norms of data flows embody an acceptable balance between fundamental rights within a given context has been criticised for its conservatism, with the danger of maintaining,

[83] H. Nissenbaum, n 10 supra, at 233; see also M. Birnhack, n 14 supra, 450, 458; R. Bellanova, 'Waiting for the barbarians or shaping new societies? A review of Helen Nissenbaum's "Privacy In Context", (Stanford University Press, 2010)', (2011) 16 *Information Polity: an international journal on the development, adoption, use and effects of information technology* 391, 393; T. Wong, 'Helen Nissenbaum's Privacy in Context: Technology, Policy, and the Integrity of Social Life (2010)', (2011) 12 *German Law Journal* 957, 965.

[84] A. Barth, Datta, JC. Mitchell and H. Nissenbaum, 'Privacy and contextual integrity: framework and applications. In: IEEE symposium on security and privacy', (2006) *IEEE Computer Society* 184; I. Agrafiotis, S. Creese, M. Goldsmith, and N. Papanikolaou, 'Applying Formal Methods to Detect and Resolve Ambiguities in Privacy Requirements', in S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, and G. Zhang (eds.), *Privacy and Identity 2010*, IFIP AICT 352 (2011), at 271; E. Toch, 'Crowdsourcing privacy preferences in context-aware applications', (2014) 18 *Personal Ubiquitous Computing* 129; G. Hull, H. Richter Lipford, and C. Latulipe, 'Contextual gaps: privacy issues on Facebook', (2011) 13 *Ethics Information Technology* 289; D. Wright, 'A framework for the ethical impact assessment of information technology', (2011) 13 *Ethics Information Technology* 199; K. Martin, 'Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract', (2012) 111 *Journal of Business Ethics* 519; N. Richards and W. Hartzog, 'Taking Trust Seriously in Privacy Law', (2016) 19 *Stanford Technology Law Review* 431; A. Selbst, 'Contextual expectations of privacy', (2013) 35 C*ardozo Law Review* 643; D. Zimmerman, 'The 'New' Privacy and the 'Old': Is Applying the Tort Law of Privacy Like Putting High-Button Shoes on the Internet?', (2012) 17(2) *Communication Law and Policy* 107.

[85] The White House, *Consumer Data Privacy in a Networked World: a Framework for protecting privacy and promoting innovation in the global digital economy*, February 2012, https://www.whitehouse.gov/sites/default/files/privacy-final.pdf . President Obama revived the proposal in March 2015, but the draft never became legislation and is now presented as a Framework, see at https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/images/Documents/Privacy%20in%20Our%20Digital%20Lives.pdf (accessed on 04 February 2017)

[86] H. Nissenbaum, 'Privacy as Contextual Integrity', (2004) 79 *Washington Law Review* 101, 124.

[87] S. Barocas and H. Nissenbaum, 'Big data's end run around anonymity and consent' in J. Lane, V. Stodden, S. Bender, and H. Nissenbaum (eds), *Privacy, big data, and the public good: Frameworks for engagement*, (Cambridge University Press (NY), 2014), 44.

[88] H. Nissenbaum, n 86 supra, 137 (her emphasis).

[89] Id. 138.

[90] H. Nissenbaum, n 9 supra, 220.

[91] H. Nissenbaum, n 86 supra, 137-138 ; H. Nissenbaum, n 9 supra, 220.

even reinforcing an 'unfair equilibrium achieved by a powerful party'.[92] However, the presumption is rebuttable and does not exclude the possibility of new practices being a better fit. Expectations of privacy derive from a 'settled rationale' as to what is acceptable within a given context but how they have been established does not preclude a renewed analysis of what the right to privacy and its limits entail because contexts have and will evolve over time. [93]

In light of her analysis of the problem, Nissenbaum proposes a framework of analysis centred around two key concepts - context and informational norms or data flows – and structured into a three-tier analysis. The first stage requires identifying in the greatest detail possible: the contexts and all informational norms, these created by the contested processing and the data flows associated with the data subjects' rights. Often, the data flows, especially the expected data flows, will be associated with the exercise of right(s). This is because a right, such as privacy, and its limits shape the boundaries between legitimate and illegitimate data flows, according to the context. Thus, all data flows and corresponding rights must be identified, whether the rights are those of data subjects, of data controllers or of third parties. CI does not equate rights to interests though: it requires outlining in great details the data flows associated with rights and interests, in order to later discuss them and notably their constitutional dimensions. This first stage allows specifying the different variables of the proportionality analysis, so that they can be weighted at the second stage. In Alexy's terminology on proportionality, this knowledge CI requires about all contextual data flows will facilitate measuring the concrete weights of rights, i.e. not only the intensity of the interference, but also the importance of the processing for the data controllers and third parties in the given context.

The second stage moves towards critically evaluating these data flows against the context's values, ends and purposes in order to determine the threats to individuals' freedoms and rights and the fairness of data protection practices. This part of the analysis will require the balancing of the various fundamental rights and freedoms that the law recognises in light of the context's ends and values as served by these rights, also taking into account the rights' constitutional dimensions (or abstract weights in Alexy's framework), as well as moral considerations.[94] The ensuing findings will help prescribe whether or not to collect, use, re-use and/or retain personal information: this will be the third and prescriptive stage. CI second stage does not provide a particular structure and some of the questions Nissenbaum puts forward may be associated more with a legislative process than with a judicial inquiry. A closer analysis of how CI second stage would fit within a court's proportionality analysis is not the focus of this paper. Rather, it centres on the first stage and the benefits it could bring to the EU legal practice in data protection.

The CI framework is not without criticisms though. Birnhack argued that CI, a normative theory defining privacy as 'a right to appropriate flow of personal information'[95], ignores that privacy defined as a right to control information 'is not insensitive to context' and recognises implicitly that there are

[92] M. Birnhack, n 14 supra, 469
[93] H. Nissenbaum, n 86 supra, 127.
[94] More maybe than Nissenbaum acknowledges, M. Birnhack, n 14 supra, 468, 471-475
[95] H. Nissenbaum, n 10 supra, 127

different actors, different purposes and transmission principles that shape data flows. Thus, the author concluded that privacy as control can be as normative as CI, even a better fit than CI in resolving conflicts.[96]

However, this paper argues that the strength of CI rests its ability to expressly identify and structure into a coherent framework the different elements upon which the weighting depends in order to be complete and precise. CI transforms the implicit into an explicit, bringing its 'descriptive rigor'[97] to provide what Birnhack acknowledged to be a 'thick and rich picture of the field at stake'[98]. The identification of context and data flows may at times not be easy, especially with regards to social media and big data that challenge the appropriateness of the concept of contexts,[99] as Nissenbaum has acknowledged and discussed.[100] Nevertheless, CI allows for a detailed factual account of both the data flows associated with the interference of a right such as privacy and of those created by the processing, in a given context. Consequently, it becomes possible to measure the intensity of interference of a right as well as of the importance of the processing for the data controller and the third parties within the context at stake.

Adopting CI as this paper proposes would not be a radical departure from actual practice. The CI first stage, based on identifying context and data flows, is largely implicit in the practice of EU data protection law. To make it explicit would facilitate the structuring of the legal inquiry in EU data protection law and of the proportionality analysis more generally.

We will now demonstrate how using CI's first element of contexts, as defined by CI, clarifies the external boundaries of the legal analysis (Part 3), and how identifying and comparing the expected data flows with those established by processing improves the assessment of interference and its seriousness (Part 4).

IV – Clarifying the external boundaries of a legal analysis: for an open and systematic integration of contexts in EU data protection law

Proportionality is contextual, thus no analysis of processing practices can take place without first identifying the contexts in which a contested processing measure sits; but context is a polysemic word, open to various interpretations. CI proposes a definition of context, thus structuring this first step of the analysis, in contrast with the intuitive approach characteristic of the DPD and of the ECJ. The GDPR represents a first step towards a more open and systematic integration of contexts in EU data protection analysis.

[96] M. Birnhack, n 14 supra, 478.
[97] H. Nissenbaum, 'Respect for Context as a Benchmark for Privacy Online: What it Is and Isn't.', (2014) *Cahier de prospective* 19, 24.
[98] M. Birnhack, n 14 supra, 464-465.
[99] M. Birnhack, n 14 supra, 469-471.
[100] S. Barocas and H. Nissenbaum, n 87; H. Nissenbaum, n 9.

A – Contexts: a defined term in the CI framework

The CI framework's key feature is its proposal of a definition of contexts in terms that will not fluctuate and that are thus applicable to any analysis of the processing of personal data. For Nissenbaum, contexts are 'the structured social systems that have evolved to manage and accomplish aspects of social life recognised as fundamental in a given society', whether these are education, the use of libraries, healthcare or commercial transactions. [101] Contexts include sub-contexts that can be shaped by the relationships between the different people interacting. For example, the general context of education includes 'universities and their distinctive substructures' as well as 'high schools', each with their own sets of actors. [102] Contexts may also overlap with some 'sectors' or 'industries' in that the latter may correspond to an identifiable context or social structure but contexts cannot be confused with them since a sector or industry may also involve several contexts[103] understood as 'abstract representations of social structures experienced in daily life'. [104]

There may be some grey areas, not easy to ascertain at first sight, but for Nissenbaum, social media or big data are not creating new contexts as some claimed.[105] In light of the definition, contexts cannot be reduced to either a technological system or platform such as a search engine, or the business model or practices of a company like Google Inc.[106] Indeed, the activities promoted by a technology are likely to correspond to multiple social domains or spheres of interaction. In particular, activities on the Internet should not be seen as pertaining to a distinct context that deserves to be analysed on its own. Online activities can be as different as shopping for a pair of shoes, checking one's bank account or reading the newspaper. 'Online activity is deeply integrated into social life in general and is radically heterogeneous in ways that reflect the heterogeneity of offline experience.' [107] Accordingly, CI requires us to identify all the contexts which online activities would pertain to if they were conducted offline. So when one uses Google to search for information, this search, if done offline, may involve different contexts, different spheres of interaction, for example interaction in a library, in a bookshop, with a financial adviser if the information searched concerns financial matters or a visit to the archives of a newspaper. Each of these contexts must be identified since each engages specific informational norms or data flows designed to serve the context's own ends and values. Indeed, in one context, a set of informational norms, and thus a form of interference with privacy, may be justified, whereas in another context the same interference with privacy would be condemned. Thus, the context shapes the contours of the analysis regarding both interference and the proportionality of this interference. This paper argues that the EU data protection framework recognizes contexts as a starting point for analysis but does so intuitively, without systematic acknowledgment and without defining contexts. By providing a

[101] H. Nissenbaum, n 10 supra, 242-243
[102] The list here is not exhaustive, see H. Nissenbaum, n 10 supra, 136
[103] H. Nissenbaum, n 86 supra.
[104] H. Nissenbaum, n 10 supra, 134
[105] M Birnhack, n 14 supra, 469-470
[106] This point is particularly clear in a subsequent article, see H. Nissenbaum, n 97 supra, 21-25
[107] H. Nissenbaum, n 9 supra, 224

definition and bringing context to the forefront of the analysis, CI provides a structure for establishing the boundaries of a legal analysis.

B - The intuitive recognition of contexts in the DPD as interpreted by the ECJ

The DPD does not use the term 'context' or define its scope or characteristics as CI does. However, the DPD's silence does not prevent us finding the concept in the interstices of the text and in its interpretation as given by the ECJ.

The closest the DPD comes to a definition of contexts in the terms used in the CI framework is in its Recital 4, which acknowledges the 'frequent recourse […] to the processing of personal data in the *various spheres of economic and social activity*' (our emphasis). The wording echoes Nissenbaum's definition of contexts as 'the structured social systems that have evolved to manage and accomplish aspects of social life recognised as fundamental in a given society'. [108] However, the DPD does not go further and the CI definition of contexts is needed to understand where contexts come into play in the DPD. For example, Article 3(2) excludes the DPD's applicability in certain situations. For the first indent of Article 3(2), the situation is that of public security, and for the second indent it is that of ordinary relationships between family and friends, also called the household exemption. These situations can be viewed as pertaining to contexts, with the EU Commission excluding them from the DPD's scope either because the Commission has no power to regulate them (Article 3(2) first indent), or because it considers there is no need to regulate the context (Article 3(2) second indent). In this respect, it is to be noted that the EU Commission's choice in Article 3(2) second indent would not be challenged by a CI analysis. As Nissenbaum concluded in her 2010 book, many accepted data flows are not regulated by the law: 'many informational norms are unsuitable for expression and enforcement in law or public policy, and in liberal democracies, certain contexts, such as *friendship*, […] as rich and important as they are, tend for the most part to be generally off-limits to regulation law and public policy'. [109] Other provisions of the DPD demonstrate awareness of contexts and their regulation. For example, Article 13(1) mentions the possibility of Member States to restrict certain data protection rights in various contexts, in particular national security (Art 13(1)(a)), defence (Article 13(1)(b)), criminal law enforcement (Article 13(1)(d)) and taxation (Article 13(1)(e)). Article 15 also refers to some contexts, for example that of employment, while Article 8 DPD, which defines the conditions for processing sensitive data, refers to the healthcare context and to the criminal justice system in Articles 8(3) and 8(5), respectively.

The list is long and it is not the purpose of this article to enumerate all contexts; rather, the above demonstrates how the CI definition of contexts can serve as a guiding light for our understanding of the

[108] H. Nissenbaum, n 10 supra, 242-243
[109] Id 236 (our emphasis).

DPD's provisions and help with appraising the ECJ's own interpretation of the DPD. CI promotes a functional approach to contexts where the traditional features of a context are indicative of its characteristics, functions and values. A particular social sphere of interaction with specific actors has evolved over time to recognise a particular set of informational norms or data flows between these actors, flows that have been developed to serve the context's ends, values and purposes. These social spheres of interaction and their associated features can evolve with time and find new forms of expression that serve the same ends, values and purposes. In *Satamedia*, the ECJ pointed towards this functional approach when interpreting Article 9 DPD, 'journalistic work'. It described journalistic activities as those the object of which 'is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them', and which 'are not limited to media undertakings and may be undertaken for profit-making purposes'[110]. Professional media do not have a monopoly over 'journalistic work' even if the context has developed around them. Other actors may be recognised as 'journalists' if, in CI terms, they fulfil the same functions and promote the values of freedom of expression in a democratic society associated with the context. [111] Therefore, contextual integrity and its related definition of context facilitate identifying where the text of the DPD, as interpreted by the ECJ, implicitly recognises context and how the ECJ intuitively proceeds to identifying the contexts at stake as a first step in its analysis.

There are, however, limits to the ECJ's intuitive approach to the recognition of different contexts. In *BL*, for which, we have seen, the ECJ was criticised, the ECJ had to interpret Regulation 45/2001 and Regulation 1049/2001 to decide the conditions upon which the names of individuals who participated in an official meeting organised by the EU Commission could be disclosed. [112] Regulation 45/2001, which reproduces the DPD, governs the processing of personal data by the institutions of the EU. In CI terms, it is a sectoral instrument that pertains to various contexts rather than just one 'structured social system […] that have evolved to manage and accomplish aspects of social life'. [113] So, for example, the Regulation can cover the context of employment of persons working for EU institutions, as well as that of the use of communications. Like the DPD, Regulation 45/2001 does not systematically recognise contexts. It falls on the ECJ to do so on a case-by-case basis. In contrast, Regulation 1049/2001 determines the conditions under which the public can access European Parliament, Council and Commission documents related to the decisions these EU institutions take. In CI terms, Regulation 1049/2001 pertains to a specific context or 'sphere of interaction', that of the decision-making process of a public institution, the public institution being the EU.

[110] Case 73/07, *Satamedia*, para 61
[111] J. Oster, 'Theory and Doctrine of 'Media Freedom' as a Legal Concept', (2013) 5 *Journal of Media Law* 57; D. Erdos, n 4 supra, 145-150 on the data protection authorities' approach the confidentiality of sources with regards to non-traditional journalists' work.
[112] Regulation 45/2001 transposes the DPD for the EU institutions. The case pre-date Regulation 1049/2001, and by the time the Regulation came to force, the case has already been heard by the General Court and the European Ombudsman. See Leino, n 49 supra, 1235.
[113] H. Nissenbaum, n 10 supra, 242-243

The ECJ acknowledged that Regulation 45/2001 deals with privacy and that there is an 'express link between [the Regulation and the Regulation 1049/2001] in Article 4(1)(b) of Regulation 1049/2001, which provides for an exception to access to a document' should there be any interference with an individual's privacy. Nevertheless, the ECJ did not go as far as identifying Regulation 45/2001 as a generic text that can apply across various contexts and that Regulation 1049/2001 seeks to regulate these contexts in complement to Regulation 45/2001. Thus the ECJ applied Regulation 45/2001 rather than Regulation 1049/2001 and required that disclosing the names of the representatives present at the meeting should be subjected to additional constraints not present in Regulation 1049/2001.[114] Consequently, the ECJ has been criticised for having discarded Regulation 1049/2001[115] as well as having established unnecessary constraints on the flow of information between EU citizens and their institutions[116].

In light of CI definition of contexts, this criticism is that of a failure to identify contexts, with cascading consequences for the ECJ's subsequent proportionality analysis. Having decontextualized its understanding of the right to privacy, the ECJ considered that a name is *always* 'private information' and should never be disclosed, whatever the context. In contrast, the GC intuitively identified the context by referring to the 'decision-making process of the public authorities' and considered Regulation 1049/2001 as the starting point of its analysis.[117] Advocate General Sharpston was even more explicit as she pointed expressly to 'the *context* (an official meeting involving representatives of an industry group acting as spokesmen for their employers, and thus purely in a professional capacity)' as one of the elements that justified her concluding that the interference was proportionate.[118] By providing a definition of contexts, CI facilitates spotting where contexts are or are not identified in various analyses and thus provides a benchmark for clarifying the external boundaries of legal analysis. *BL* is a case in point, illustrating how crucial contexts are to analysis, since the initial failure to identify the correct contexts led the ECJ to identify incorrect data flows. In this sense, the case demonstrates that the ECJ's intuitive recognition of contexts is not sufficient: there is a need to integrate the concept of context (as understood by Nissenbaum) openly and systematically into legal analysis in data protection law.

C – The GDPR's more open approach to contexts

Viewed in light of CI, the GDPR does not simply reproduce the DPD's approach to contexts. Unquestionably, as its core principles are modelled on the DPD, a number of its articles that mirror the DPD do not use the word 'context' either and yet pertain to it. However, the main change the GDPR introduces is the use of the word 'context' in eight Articles and two Recitals. The two Recitals use the term as part of their guidance on two of the currently controversial grounds for processing: further

[114] Case 28/08 P, para 78
[115] P. Leino, n 49 supra, 1238
[116] Id 1238, 1239, 1247
[117] Case 28/08 P, para 98
[118] (our emphasis) Case 28/08 P, Opinion AG, EU:C:2009:624, para 192

processing and the legal ground of Article 6(1)(f) GDPR, equivalent to current Article 7(f) DPD, featuring in a number of the ECJ's decisions, as discussed above. [119] Significantly, the Recitals' wording echoes part of CI's own definition. Context is referred to with regard to 'in particular […] the relationship between the data subjects and the controller'[120], i.e. with regard to the interaction of actors, which CI considers to be indicative of the context's characteristics and scope as a 'social sphere of interaction'. Therefore, in light of CI's definition of context, these references to contexts can be understood to be the particular application of a general criterion critical to legal analysis. Despite the GDPR having no generic 'respect for context' clause like that in the 2012 US Consumer Bill, drafted with express reference to CI, it represents a more open approach than the DPD. It can also be viewed as a step forward that could provide strong legislative support for the ECJ's current approach to context. The ECJ could draw on these references to contexts to use the concept expressly and systematically whatever the grounds of processing, using CI definition of context as a benchmark.

Even if contexts were integrated fully into legal analysis, this important step will not suffice to guarantee a full assessment of the interference that a processing measure creates. Another element of the CI analysis should be recognised: the use of informational norms to identify contextually *all* data flows to be discussed during the proportionality analysis.

IV – For a better determination of the intensity of the interference and the importance of the processing: the need for a contextual determination of all data flows based on CI

Once the contexts are identified, contextual integrity requires describing all data flows or informational norms. To ensure the comparability of data flows, CI provides three common elements to identify the flows: actors, data types and constraints on the flows. To facilitate the completeness of the analysis, CI requires examining *all* data flows *contextually*. Whilst both the DPD and GDPR share the definition of data flows with CI, neither contains an express and general requirement to identify all data flows bearing in mind the contexts identified. Subsequently, the ECJ finds it difficult to identify contextually *all* data flows in great detail under the DPD. These difficulties lead to the criticisms of the ECJ's decisions, and echo more general concerns about the proportionality analysis. To incorporate CI formally would improve the determination of the intensity or seriousness of the interference, as well as the understanding of the degree of importance of the processing for the data controllers and for third parties.

A – Ensuring comparability: the CI definition of data flows in the DPD and GDPR

[119] Case 131/12, *Google Spain*; Joined Cases 468/10 and 469/10, *Asnef*.
[120] Recitals 38 and 40

Because rights and their limits generate data flows, understanding these respective data flows and how the flows compare is facilitated where the same grid of analysis is used. The DPD and GDPR share with CI the three parameters of data flows (CI informational norms): actors, data attributes and transmission principles.

Actors in CI are of three types: the information subject, the sender of information and the recipient of information. They can alternatively be senders and recipients; for example, when the recipient of the data subject's information shares this information with third parties, s/he becomes a sender. CI requires the identification of *all* actors involved in the flow of information so as to determine the capacities in which they interact within a particular context.[121]

The DPD and GDPR identify five types of actors: data subjects (definition inferred from Article 2(a) and (h) DPD, Article 4(1) GDPR), data controllers, data processors, recipients and third parties, (defined in Articles 2(d), 2(e) 2(g) and 2(f) DPD (Article 4(7)(8)(9)(10) GDPR, respectively). Viewed in light of the CI decision heuristic, the two texts recognise various recipients, using four terms to describe them: data controllers, data processors, recipients and third parties. The distinction between the four types of recipients reflects differences in the rights and obligations attached to each. [122] In CI terms, this is a difference in the transmission principles to which each actor is subjected. These categories of recipients are determined according to who the senders are. The data subject him/herself will be one sender to a main recipient, i.e. the data controller, and the data controller can in turn become a sender with regard to other recipients of information, be they third parties, data processors or recipients. Neither DPD nor the GDPR require the express identification of senders. From a CI point of view, the danger could lie in forgetting to map the data flows between the different recipients and senders, which in turn would undermine the quality of the analysis when evaluating the informational norms.

Invariably, the identification of relevant actors leads to the determination of the data attributes or information types, i.e. the types of data that flow between senders and receivers. To define these data attributes, Nissenbaum quotes the text of Article 2(a) DPD. [123] Thus, there is a full correspondence between the DPD and the CI framework. The ECJ has adopted a wide interpretation of Article 2(a) DPD, with data including IP addresses and even work hours. [124] With its Article 4(1), the GDPR confirms the DPD definition, adding that identifiers can include location data, online identifiers and other elements by which the person is identifiable.

[121] H. Nissenbaum, n 10 supra, 141-142

[122] Article 29 Working Party (2010), *Opinion 1/2010 on the concept of 'controller' and 'processor'*, WP 169, Brussels, 16 February 2010, at 31

[123] H. Nissenbaum, n 10 supra, 4-5

[124] Case C-342/12, W*orten – Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT)* OJ C 225, 03/08/2013, 37. But not the legal reasoning supporting a decision on residence, Joined Cases 141/12 and 372/12, *YS* v *Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v M and S*., [2015] 1 C.M.L.R. 18; Case 582/14, *Breyer v Bundesrepublik Deutschland*, OJ C 475, 19/12/2016 p. 3

Data attributes differ from transmission principles. The latter are the terms and conditions under which the flow of data ought (or ought not) to occur.'[125] Transmission principles can indicate a free flow of information just as much as a very restricted flow or no flow at all when the information is not revealed to others. For Nissenbaum, a variety of constraints regarding disclosure exist and can be used concurrently or separately: confidentiality (no sharing with third parties), reciprocity, entitlement (to information), compulsion (data subject is legally compelled to reveal information), need (one party needs to know a particular set of data elements), knowledge of data subject (notice by privacy policy) or permission (consent).[126] Means of recording, time and space can also be seen as constraints and thus transmission principles: our flimsy memory of passers-by in the street establishes a constraint different from that of the more permanent recording of the same people passing made by CCTV.

The DPD and GDPR first determine what forms transmission can take, with the concept of 'processing' defined in Articles 2(b) and 4(3), respectively. The scope of processing is vast and, so far, the ECJ has confirmed that the DPD applies to a variety of situations ranging from collection, recording and storage to the dissemination of personal data through a search engine, phonebooks, a website or a text-message. [127] The DPD and GDPR then express a variety of constraints that apply to the transmission process between senders and recipients. The standard transmission principles are expressed in Articles 6 and 7 DPD (Art 5 and 6 GDPR), with Article 8 DPD (Art 9 GDPR) establishing more stringent constraints for the data identified in 'special categories'. The rights of the data subject as expressed, for example, in Articles 10 and 11 DPD/Article 12 GDPR (information) or in Articles 12DPD/15GDPR (access), can also be seen as establishing constraints and thus transmission principles. Thus the DPD provides a detailed framework for transmission principles and their use, with the GDPR confirming the core elements.

However, identification of transmission principles, as well as of data attributes and actors, is not in itself sufficient. CI also requires all three parameters of data flows to be identified *within* their contexts for the proportionality analysis to be complete and precise.

B – Ensuring completeness of analysis (1): the need for the contextual identification of data flows

'Usually, when we mind that information about us is shared, we mind not simply that it is being shared but that it is shared […] with *inappropriate* others'. [128] 'Appropriateness is not one-dimensional nor is it binary'[129]. In particular, the nature of the data sets does not dictate *per se* and *in abstracto* the appropriateness of the information flow and the choice of transmission principles. Context plays a critical role here. Within the same context, different types of data may be treated differently but the

[125] H. Nissenbaum, n 10 supra, 145
[126] H. Nissenbaum, n 10 supra, 145.
[127] Case 73/07, *Satamedia* and Case 131/12, *Google Spain*.
[128] H. Nissenbaum, n 10, 142 (our emphasis).
[129] Id. 144

difference is justified by the context, not just by the nature of the data assessed. Different contexts may also call for different transmission principles to apply to the same type of data. For example, the same data - religious beliefs - have two different transmission principles attached to them, according to the context at stake: they will be usually 'off limits in a job interview or workplace' but appropriate subjects for discussion within a friendship. [130] Consequently, for Nissenbaum, categorising information types into, for example, sensitive data, private data and public data, may lead us to conflate the nature of the data with the transmission principles attached to the data. In the process we may forget the context that governs these elements of the data flows.

In this respect, both the DPD and the GDPR avoid this error and do not distinguish on the basis that the data are 'public' or 'private'. Despite their use of the expression 'sensitive data' in their Recitals[131], the wording corresponds to the identification of different transmission principles according to the context implicitly at stake in Articles 8 DPD and 9 GPDR. To take the above example of religious affiliation, Article 8(2)(d) DPD, future 9(2)(d) GDPR, forbids a religious organisation to disclose this 'sensitive' data to third parties without the consent of the individual concerned but Article 3(2) DPD, future Article 2(2)(c) GDPR, leaves the disclosure of this form of personal data unregulated in the context of a purely personal or household activity. Thus, the two texts avoid the danger of decontextualizing the choice of transmission principles.

The corollary of this interdependence between contexts and the identification of the three elements of data flows is that any interpretation of the DPD and GDPR must avoid imposing the transmission principles previously attached to a data set on the same data set without first undertaking a reassessment of context. In two cases the ECJ intuitively followed this interpretation and required context to be integrated into analysis when identifying data flows.

In *Satamedia*, where the company Satamedia reproduced tax data already 'in the public domain under national legislation', the ECJ considered that the previous publication of the documents by national authorities did not exempt Satamedia from complying with the rules set out in the DPD. Otherwise, 'it would be sufficient for the Member States to publish data in order for these data to cease to enjoy the protection afforded by the Directive'. [132] Data published does not equate to data available at any time, whatever the context, and without a subsequent reassessment of the balance of fundamental rights that the context would call for. Since Satamedia argued it operated within the 'journalistic work' context of Article 9 DPD, its processing of the data needed to be reassessed with regard to that context, which is precisely what the national courts did after the ECJ defined the concept of 'journalistic work' in its decision. [133] Further processing of data is possible but not on the sole basis that others have initially published the data.

For the same reasons, 'private data' cannot lead to a blanket exclusion of the use of data whatever the context. It is the context that will shape the discussion and indicate the boundaries between

[130] Ibid.
[131] Directive 95/46 Recitals 34 and 70; GDPR Recitals 10 and 51
[132] Case 73/07, *Satamedia*, para 48
[133] For the details of the national courts' assessment, see ECtHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland*, Appl. No. 931/13, judgment of 21 July 2015; and in Grand Chamber, judgment of 27 June 2017

legitimate and illegitimate data flows, not the nature of the data types per se. In *Asnef,* where Spain, in its transposition of Article 7(f) DPD, imposed a blanket ban on the use of private data, the ban decontextualized the data sets and their related transmission principles. By rejecting the ban, the ECJ implicitly established that Article 7(f) DPD requires the context to be identified because the informational norms, especially the transmission principles and the types of data, are likely to differ according to context. [134] The ECJ's judgment was criticised for its 'factual effect of legitimizing' the use of consumer financial data by commercial credit bureaus and marketing agencies in Spain[135]. However, CI shows that nothing in the ECJ's interpretation of Article 7(f) DPD forbids the Spanish legislator from banning the use of this type of data by those actors as long as it establishes the ban contextually with context-specific informational norms that will reflect a balancing of rights and interests in light of the context's ends, values and purposes.

Therefore, the ECJ's interpretation in these two cases implicitly promoted a contextual approach to determining appropriate constraints on the flow of specific data sets. This approach is not specific to the grounds of processing it was asked to interpret but concerns all processing to which the DPD and GDPR apply. To improve the analysis, it must be formalised. The additional challenge for the ECJ lies in accepting to describe *all* data flows fully and systematically, not just the flows introduced by the processing with a short, at times vague, comparison with the expectations of the data subjects.

C – Ensuring completeness of analysis (2): the need for systematic determination of *all* data flows

In light of CI, most of the criticisms directed at the ECJ's decisions can be viewed as the ECJ's difficulties in systematically describing all the data flows at stake, in the absence of a formal requirement in the DPD. When the ECJ was criticised for not having identified the right associated with the legitimate objective for processing or for not having explained what interference with the right to privacy entailed in terms of intensity, in effect the ECJ was criticised for not having outlined the contextualised data flows created by the processing as well as those expected by the data subjects in the context being considered and embodying their right to privacy. CI does not put forward a judgement of value as to the respective constitutional context of the rights and interests at stake. Rather it posits that the constitutional context cannot be discussed without first outlining in great detail all the data flows. For example, in *Schecke,* where the ECJ was criticised for not having linked the legitimate objective of transparency pursued by EU institutions with data subjects' right to access documents as protected in the Charter, it was also pointed out that the ECJ did not explain that different conceptions of transparency would call for different data flows, and thus did not enquire as to "what type of transparency is acceptable and how is to be balanced in the individual case". [136] Assumptions concerning the measure in question (Alexy's epistemic factor) were not discussed.

[134] Joined Cases 468/10 and 469/10, *Asnef*, paras. 40, 44-45
[135] F. Ferretti, n 47 supra, 864
[136] M. Bobek, n 48 supra, 2015-2016.

In *Google Spain*, to determine how processing interfered with the right to privacy, both the Advocate General and the ECJ began by identifying the new data flows established by Google's processing in terms of actors, data sets and transmission principles, although they did not use this terminology. Then, they highlighted how these new data flows represented a change in practice by implicitly comparing these flows with past practices and expectations of data flows. The ECJ noted that the list of results was now 'ubiquitous': 'any internet user' could obtain 'information which potentially concerns a vast number of aspects of [an individual's] private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty.'[137] The Advocate General also recognized the 'universal accessibility of information on the internet search engines', whereas in the past 'finding relevant information without them would [have been] too complicated and difficult and would [have] produce[d] limited results'. [138] The Advocate General was even more precise than the ECJ as he indicated his agreement with the Spanish court's observation that 'acquiring information about announcements on the forced sale of the data subject's property would previously have required *a visit to the archives of the newspaper*' (our emphasis) with the correlative restrictions in time and physical access that this past practice incorporated. [139]

However, neither the Advocate General nor the ECJ articulated in more detail what the data flows generated by past practices were and how they embodied the balance so far applied between the right to privacy and freedom of expression. Thus it became impossible for them to compare the two sets of data flows effectively and take the measure of the intensity of the interference as well as the importance of the processing promoted by Google. Time, allied with physical constraints, had in practice created the conditions for information to be forgotten. Never expressly articulated, they nonetheless shaped the expected data flows and led to a certain balance between the right to privacy and freedom of information. For example, with the passing of time – here, sixteen years as the ECJ noted[140]- some materials originally located in local libraries would have become unavailable and would have required visiting other locations. In England, to consult old newspapers without Google, and before the materials were digitised, one would have needed either to go to the British Library Newspapers Room and use microfiches or to visit the archives of the newspaper and painstakingly search through them. With search engines, access to, and aggregation of, information becomes available at a click, at any moment, by anybody, from anywhere and across contexts. This new processing challenges our expectations of privacy built on past constraints of time and physical location that have since disappeared. How the balance between privacy and freedom of information must be set depends on identifying the two essential elements of the discussion: the temporal and spatial constraints on the expected data flows, and the facilitated access to aggregated information with the new data flows.

Yet, the Advocate General and the ECJ both missed one key aspect of the discussion. Time constraints (but not physical locations) were the main focus of the ECJ's decision, whereas Advocate General Jääskinen did not analyse these restrictions despite having noticed the constraints of

[137] Case 131/12, *Google Spain* para 80
[138] Opinion, EU:C:2013:424, paras. 45, 78
[139] Id, para 45
[140] Case 131/12, *Google Spain* para 98

location.[141] On the other hand, the Advocate General expanded considerably on freedom of information and the crucial role of search engines in allowing access to information. [142] By not identifying in great details the data flows and associated rights which exercise the processing under Article 7(f) DPD facilitated, the ECJ was not able to discuss later how the increased flow of data created by Google's processing contributed to users' freedom of information. Should the contextual identification of *all* data flows have been integrated into their analyses of what the interference was, the Advocate General and the ECJ would have then been able to articulate, in detail and in equal measure, their relationship in the proportionality analysis.

Furthermore, failure to use the CI structure to identify all data flows may lead to establishing transmission principles that will not be appropriate constraints on the flow of data. In *BL*, the ECJ not only omitted to refer to context but also did not identify the data flows constituting expectations of privacy, with the consequence that it added further restrictions to the flow of data. Yet the data flows that the right to privacy and its limits generated within the context were implicitly part of the discussion in the first instance. The GC concluded that the publication of names in the meeting's minutes did not interfere with the right to privacy because the individuals, the disclosure of whose names was requested, 'participated in the meeting as representatives of the bodies to which they belonged'. [143] In CI terms, the GC's wording referred to the expected norms embedded in the context. The transmission principle of disclosure has become so entrenched in the context that the GC has forgotten that disclosure potentially interferes with privacy but that this interference has been justified and accepted. If the GC had followed the CI framework of analysis, it would have had to identify all data flows, those entrenched in the context and those which Bavarian Lager requested that the Commission apply. The comparison would have revealed that Bavarian Lager's request to see all the names of the individuals present at the meeting was rather in line with standard practice and expected data flows. The GC could then have enquired about the proportionality of the processing measure and determined whether it could be justified for the same reasons as before. This is in essence what Advocate General Sharpston did, explaining that disclosing the names, despite interfering with the right to privacy, was justified under Regulation 1049/2001.[144] Thus, CI reinstates some meaning into the different analyses conducted in *BL*, providing an explanation for why the ECJ's decision was criticised. CI also shows that even where contexts are identified, as in the GC's decision, given that the DPD does not point to the specific identification of contextual *entrenched* norms shaping our expectations of privacy it may be difficult to explain these expected data flows and to articulate them with regard to the contested data flows. Following the CI analytical structure acts as a safeguarding mechanism, allowing us to establish all the elements that need to be discussed at the later stage.

Given the weaknesses of the DPD and of the ECJ's approach to this matter, it would be welcome news if the GDPR were to provide some clarification over the identification of the data flows. The text is slightly clearer in that it expressly requires the expectations of data subjects about data flows to be

[141] Opinion, para 111. He considered that Directive 95/46 does not provide for a right to be forgotten.
[142] Opinion, paras. 120-135
[143] Case T-194/04, para 125
[144] Case 28/08 P, Opinion, paras. 188-193

taken into consideration in the analysis in Recital 49, pertaining to Article 6 (1)(f) GDPR equivalent to Article 7(f) DPD, and in Recital 50 related to Article 6(4) on further processing. Thus, the GDPR formalises the ECJ's intuitive approach to the contextual determination of all data flows in its cases interpreting Article 7(f) DPD.

What the GDPR does not state explicitly though is that this determination is not specific to the two types of processing it mentions. Whatever the ground for processing, the expected data flows should be identified and compared with the data flows created by processing. Therefore, whilst the GDPR represents the way forward, because the text falls short of establishing a general requirement to analyse all data flows, it would require adopting CI as a framework of interpretation.

VI - Conclusion

The key challenge that this paper addressed was how to establish the boundary between legitimate and illegitimate processing of personal data consistently and transparently. It argued that a more satisfactory approach to interpreting the DPD and the future GDPR exists. Using the contextual integrity framework developed by the US social scientist Nissenbaum provides an effective and objective analytical framework that brings together the various elements of the discussion in the DPD (as interpreted by the ECJ) and GDPR, and better structures the proportionality analysis.

CI's requirements of identifying context and all data flows already implicitly underpin the analysis in the DPD and its interpretation by the ECJ. However, in some cases, the lack of systematic integration of the framework has led to difficulties for the ECJ in stating the elements of a problem, with cascading consequences for the proportionality analysis. In Alexy's terminology, the intensity of the interference and the degree of importance of the processing for the data controller and for third parties cannot be precisely identified, and thus it becomes difficult to ensure that 'the more heavily an interference with a constitutional right weighs, the greater must be the certainty of its underlying premises.' As the wider debate on proportionality indicates, a proper proportionality assessment is contextual. Context, for which CI provides a definition, precedes the entire legal analysis and thus must be systematically identified whatever ground of processing the data controller chooses. Furthermore, because the data flows form the factual matrix on which the proportionality assessment depends, CI structures the discussion on rights that will take place at the weighting stage by requiring the identification of the data flows and the associated rights. Concrete weights of rights can be identified and measured.

Consequently, this paper recommends that the legal analysis in EU data protection law adopts a three-tier structure instead of the current two-tier structure. The first and new step should aim to clarify the external boundaries of the legal analysis by identifying the contexts that CI defines as 'social spheres of interaction'. The second and third steps, previously first and second, should ensure that all data flows are identified in terms of actors, data types and constraints on the flow of information. It is not enough to identify the rights at stake in the analysis, whether they relate to the purpose and legitimate objectives of data controllers and/or third parties, or whether they are the data subjects'

rights that processing interferes with. All data flows must also be described in great detail: the flows of data created by the new and contested processing measures and the expectations of data flows that a right generates with a context. These three preliminary steps would enable the identification of all the factors necessary to assess proportionality at the last stage. The resulting analysis in EU data protection law would be stronger, more consistent and less open to manipulation and arbitrariness concerning the various steps to be undertaken, whether by the ECJ, its Advocate Generals or by other decision-makers, specifically data controllers. There is no need to abandon the proportionality principle in data protection law as recently suggested. CI allows taking proportionality seriously.

With its express references to contexts and the expectations of data subjects in a number of Articles and Recitals, the GDPR, which is likely to have been partially inspired by CI, legitimises the ECJ's intuitive approach. It is too early to tell whether or not the GDPR will succeed in supporting the ECJ's future decisions and restoring the trust of all stakeholders in the digital environment, as it aims to do. Nevertheless, this paper considers that the GDPR has the potential to do so, providing it is interpreted in light of CI. Should the GDPR be revised, EU institutions could benefit by openly integrating the CI structure and descriptive rigor of its first stage.

Further, since rights do not exist in a vacuum and their limits are set with regard to a context, it may also be that CI, with its contextual analysis of all the data flows generated by a right, could apply outside the field of data protection law, for example when there is a conflict in rights analysis between freedom of expression and the right to privacy. The right to privacy, which overlaps but is not to be conflated with the right to data protection, has been acknowledged to be contextual, like any proportionality analysis. What context means and how it shapes rights and their limits remains to be explored further in light of the contextual integrity framework.