Putting Consent in its Place: Proceduralism and Paternalism in EU Data Protection Law

Shukri Shahizam*

ABSTRACT

It is highly likely that any discussion on EU data protection law begins with the notion of consent. Yet, this carries the danger that a disproportionate load is placed on consent as a regulatory tool. This letter argues that although consent can – and should – play an important role in conceptualising data protection, reliance on consent cannot be to the extent that it overshadows substantive restrictions on data processing. Instead, regulators should grasp the nettle and accept that modern asymmetries between data subjects and data controllers make paternalistic approaches to data protection a necessity.

* LLB (LSE) '19; LLM (Cantab) '20. The author was the Editor-in-Chief of the LSE Law Review during the 2018/19 Academic Year Board.

Dear Editor,

'Consent' rightfully occupies a central role in the normative justification for the existence of data protection law ('DP law'). However, the extent of DP law's restrictions on the processing of personal data should not be equated with consent-based restrictions. Normative priority given to consent in EU DP law is *justifiable* given that Article 8 of the Charter of Fundamental Rights ('CFR') makes express reference to consent. However, consent has played too large a role in the legitimation of data processing, notwithstanding the imposition of requirements imposed on 'true' consent. Examples include the General Data Protection Regulation's ('GDPR') conditions for consent contained within its definition in Article 4(11) and the role of consent in promoting the extensiveness of transparency rules. Accordingly, it will be argued that data protection ought to move away from its proceduralist preoccupation with consent and transparency and focus on substantive restrictions on the use of personal data that requires regulators to shed the fear of paternalism.

On the face of it, data subject consent is merely one of six legal grounds for the processing of personal data provided by Article 6(1) GDPR.[1] However, this belies the more extensive normative role that consent plays, if not in the formulation of legal grounds, then in the extant 'notice and consent' paradigm of DP law.[2] To a limited extent, this focus is justified: the new fundamental rights *vires* for data protection in the EU – Article 8 of the CFR – expressly states that personal data 'must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.[3] Thus, despite the presence of other grounds for the lawful processing of personal data under the GDPR, a continued perception that consent is *primus inter pares* is unavoidable.

[1] Regulation 2016/679 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 (GDPR) (2016) OJ L119/1, art 6(1).
[2] Fred H Cate, 'The Failure of Fair Information Practice Principles' in Jane K Winn (ed), *Consumer Protection in the Age of the Information Economy* (Ashgate 2006).
[3] Charter of Fundamental Rights of the European Union (2012) OJ 1 326/391, art 8(2).

This is manifested in practice as the vast majority of personal data is processed on the basis of data subject consent. All other grounds for processing are subject to twofold substantive restrictions: first, by the 'necessity' requirement on the face of the ground; and second, through the data minimisation principle under Article 5(c). Although data processed with consent is also subjected to data minimisation, the purpose for which consent is acquired can be expanded to render moot any protection provided by the principle. Accordingly, the consent ground allows for a far greater scope of purposes for which controllers may legally process data, giving it a central role in practice. In the previous regulatory regime under the Data Protection Directive ('DPD'), the predominance of user consent was expressly flagged by Article 29 Working Party – the EU advisory body established under by DPD – as an area of concern. This was due to data controllers' unnecessary use of consent where other, more limiting, grounds would be better suited to the relevant circumstance.[4]

The prioritisation of consent as a regulatory lodestar is evident when the GDPR is considered on the whole. The principles relating to the processing of personal data in Article 5 intimate an approach to data protection that has a substantive focus – e.g., in the principle of purpose limitation, data minimisation, and accuracy. Yet, the remainder of the GDPR, as a rule-based framework, appears to be firmly proceduralist in its inclination. Therein, 'consent' is emblematic of a broader regulatory posture that focuses on the responsibility of the data subject as an active participant in the protection of their own personal data. At the outset, the apparent stringency of Article 4(11) prescribing that consent to data processing be 'freely given, specific, informed and unambiguous' obscures the imposition of a regulatory burden on the data subject.[5] Despite restricting the mechanisms through which potential data controllers may receive consent, the substantive efficacy of those requirements is dependent on the potential data subject's active participation. In other words, such restrictions are only restrictions *in practice* if the subject is sufficiently informed and has sufficient ability to consider the consequences of data processing and to, if necessary, withhold consent.

[4] Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent* (WP187, 01197/11/EN) 10.
[5] GDPR, art 4(11).

Hence, within the overall scheme of DP law, an understanding of the role of 'consent' must also consider its essential relationship to the notion of, per the Working Party, 'informational self-determination'.[6] Conceived in this way, the normative justification for consent is shared with that of the extensive GDPR provisions relating to transparency and control in Articles 12-22. Proactive transparency under Article 13 can be traced back to the notion of informed consent, whereas modalities of control rights under Articles 15-22 can be associated with the notion of ongoing consent where, per Article 7(3), the data subject has a 'right to withdraw [their] consent at any time'.[7] As with the conferral of consent itself, the efficacy of these provisions in protecting personal data is dependent on the data subjects themselves exercising their regulatory agency.

The importance given to consent, broadly understood, in the context of data protection is not inherently problematic. What *is* given importance is consent's priority over substantive restrictions on data processing, namely prohibitions on certain forms of processing. The focus on informational self-determination – in the form of consent, transparency, and control – makes the GDPR's centralisation of consent vulnerable to the same criticism Cate makes of the fair information practice principles. That is, there is an inappropriate substitution of consumer choice in place of more direct protections of the consumers' interests. Although Cate's criticism focuses on the disappearance of the protection of data subjects' privacy interests,[8] the general absence of privacy in the GDPR means that the normative focus in EU DP law should shift to the protection of personal data per se. Of course, this has a robust legal basis given the presence of the right to personal data protection in primary EU law via Article 16 TFEU and Article 8 CFR.

Quelle persuasively argues that the prevalence of the consent, notice, and control paradigm stands in the place of more interventionist regulations, which would address data protection interests paternalistically.[9] To a large extent, such

[6] Article 29 Data Protection Working Party, 9.
[7] GDPR, art 7(3).
[8] Cate (n 2) 357-9.
[9] Claudia Quelle, 'Not Just User Control in the General Data Protection Regulation: On the Problems with Choice and Paternalism, and on the Point of Data Protection' in Lehman and others (eds), *Privacy and Identity Management: Facing up to Next Steps* (Springer 2017) 146.

mutual exclusivity is real. An imposition of substantive restrictions on certain forms of data processing is a limitation of data subjects' personal agency to consent to that processing. Doing so requires giving normative precedence to the interest justifying substantive restrictions over the data subject's ability to do as they wish with their data. This concession to paternalism, no matter how marginal, necessarily undermines a consent-absolutist approach which holds that any form of data processing can be made legal if accompanied by an appropriate degree of notice and consent.

Yet, the necessity of paternalism in itself should not be seen as determinative of a reason why a firm movement away from consent is undesirable. Indications of a willingness to isolate certain forms of data and processing as carrying a particular risk are already evident in the GDPR's regimes relating to special data and rules relating to impact assessment. Although the concept of sensitive or special data has been a consistent feature in EU DP law since its inception, it is no less significant insofar as its existence as an area which, per the Working Party, has been given particular regulatory attention on the 'presumption that the misuse of [sensitive data] could have more severe consequences on the [data subject's] fundamental rights, such as the right to privacy and non-discrimination than misuse of other, "normal" data'.[10] Therein lies an acknowledgement that there *is* a proper role for regulators to integrate within the regulatory regime structures which factor in the potential consequences of misuse. This stands in contrast to a stance which shifts the cognitive load onto the data subject in relation to their exercise of their power to give consent and, later, in the exercise of transparency and control rights. Although the impact assessment regime under Articles 35-36 is primarily procedural, it contains elements of a more substantive and paternalistic approach to regulation in the presence of Article 35(3), which prescribes certain instances where an impact assessment is necessary, specifically where there is 'automated' and 'systematic and extensive evaluation' of personal information, 'processing on a large of [special data]', or 'large scale' 'systematic monitoring of a publicly available area'.[11]

[10] Article 29 Data Protection Working Party, *Advice Paper Ron the special categories of data ('sensitive data')* 4.
[11] GDPR, art 35(3).

Both the sensitive data regime and the isolation of specific processing-related activities for special regulatory scrutiny exhibits the seeds of, per Mayer-Schönberger and Cukier, a DP framework that is 'focused less on individual consent at the time of collection and more on holding data users accountable for what they do'.[12] Such an adjustment to the normative priorities in DP law would be justified on the basis of the significant factual overlap between the entities that process large amounts of data in largely opaque and potentially objectionable ways and those whose consent is binary, insofar as their terms are non-negotiable. Key examples of entities are, of course, those which constitute the infrastructure of the internet like social media companies and search engine operators. Despite the recognition in Recital 43 GDPR that instances of a 'clear imbalance' between the controller and subject can cast into doubt whether consent was given 'freely',[13] this recognition is insignificant insofar as it does not manifest in paternalistic approaches which are more willing to intervene and nullify the validity of consent or, as stated before, impose additional substantive restrictions on top of consent.

In conclusion, although consent has a rightful place at the core of DP law, its prominence should not be over-stated and over-applied. Instead, it must be accepted that the current context within which DP law exists means that consent and its attendant notions of notice and control should be supplemented by more interventionist regulations on the use of personal data. Although this adjustment would be significant, it would not be excessively foreign, given that the largely proceduralist GDPR contains indications of a willingness to pass judgement on specific forms of data processing and, accordingly, impose heavier regulatory burdens on controllers who partake of them.

Yours sincerely,

Shukri Shahizam

[12] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt 2013) 173.
[13] GDPR, recital 43.