Not just User Control in the General Data Protection Regulation

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

Claudia Quelle

Tilburg Institute for Law, Technology and Society; Tilburg University
c.quelle@tilburguniversity.edu

Keywords: data protection · controller responsibility · informational self-determination · consent · paternalism · fundamental rights

Abstract. User control is increasingly prominent in the discourse surrounding the General Data Protection Regulation (GDPR). However, alongside user control, the GDPR also tries to achieve what will be called controller responsibility. Is this unjust paternalism or does it correctly place the responsibility for data protection with the controller and its supervisory authority? This paper argues that the question of responsibility should be evaluated in light of the overarching objective of the GDPR to protect the fundamental rights of natural persons. It describes the problems of a focus on the "choice" of data subjects, but also takes seriously the charge of paternalism which more protective data protection laws are faced with, tying the resulting dilemma to the objectives of data protection and ultimately to the debate on the nature of rights. Does data protection law seek to protect certain interests, such as secrecy and seclusion, or does it seek to give data subjects control over their data, and thereby political power regarding the substance of their fundamental rights? The paper concludes that a further exploration of will theories and interest theories of rights would shed light on the appropriate roles for user control and controller responsibility.

1 Introduction

Should the General Data Protection Regulation (GDPR) serve to give data subjects control over the information pertaining to them, or should it require controllers to protect data subjects? This paper argues that the GDPR emphasizes and strengthens the rights to control of data subjects, but also seeks to reinforce the fairness and due care exercised by the controller. Throughout the paper, controller responsibility is contrasted with user control [cf 1]. Controller responsibility covers the notion that it is up to the primary norm-addressees of the GDPR — the controllers — to ensure, through fair data processing practices, that the objective of data protection law is met. Controllers have to ensure that the fundamental rights of natural persons are protected in the context of personal data processing, irrespective of whether data subjects put

forward any claims or demands. The tenet of user control seeks to give data subjects a measure of influence over the way in which their fundamental rights are protected, typically by granting them the power to demand certain protections or to shield themselves from certain intrusions.

According to van der Sloot [3], data protection law originally posed principles of good governance. Recently, however, there is an increased focus on the individual and her rights of control. Scholars like Purtova [3] would consider it radical to reject informational self-determination as 'a foundation of the European approach to data processing'. At the same time, the tenet of user control has been subject to scrutiny lately, as it is increasingly recognized that current notice-and-consent practices do not empower the average data subject in a meaningful way. This has lead Matzner et al [4] to speak of *responsibilization*, defined as 'the process whereby subjects are rendered individually responsible for a task which previously would have been the duty of another — usually a state agency — or would not have been recognized as a responsibility at all' [5]. Matzner et al argue that the state should be responsible for granting citizens data protection. Indeed, on the one hand, data subjects should not be burdened with the task of safeguarding the protection of their personal data, preventing that the processing operations of controllers bring about unwanted consequences. On the other hand, there might be something about data protection which requires the involvement of data subjects — e.g. to prevent abuses of power and to define the boundaries between the permissible and the impermissible in the first place.

This paper deepens the debate by tying it to the nature of rights in general. Is the protection of the fundamental rights of individuals something which controllers, under the supervision of supervisory authorities, could take on for the benefit of the rights-holders? The paper does so in three parts. The following section will examine the presence of the two tenets of user control and controller responsibility in the GDPR. Next, section three explores the virtues and drawbacks of a user control approach, taking seriously Solove's worry regarding paternalism. Section four looks into the objectives of data protection law and proposes that the question of responsibility should be evaluated in light of the overarching objective of the GDPR to protect the fundamental rights of natural persons. A dilemma is found: fundamental rights protection by others than the data subjects themselves is (at best) based on the way in which their interests are perceived. However, the alternative is to require them to express their interests and their opinions on what counts as an appropriate or an inappropriate collection or use of personal data, which might impose too high a burden**.** The debate between interest-based and will-based theorists is identified as a possible area of research to investigate the legitimate roles of user control and controller responsibility.

2 The General Data Protection Regulation

The GDPR has been increasingly presented as an instrument which seeks to strengthen user control, although another major drive of the reform was to strengthen the responsibility and accountability of controllers. At the start of the reform process in 2009 and 2010, the Commission [6] and the Article 29 Working Party [7] sought to

strengthen the rights of data subjects, but also explored 'ways of ensuring that data controllers put in place effective policies and mechanisms to ensure compliance with data protection rules' [6]. Controllers should show how responsibility is exercised and make this verifiable; '[r]esponsibility and accountability are two sides of the same coin and both essential elements of good governance' [8]. This is how the obligations to conduct a data protection impact assessment, implement data protection by design, and appoint a data protection officer came to be. While the Impact Assessment of 2012 [9] does discuss these accountability mechanisms, the problems it identifies with regard to the Data Protection Directive are only (1) 'barriers to business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement' and (2) 'difficulties for individuals to stay in control of their data'. The Impact Assessment laments that 'individuals are often neither aware nor in control of what happens to their personal data and therefore fail to exercise their rights effectively'. At this point in time, also the Commission [10] talks about putting individuals in control of the data pertaining to them. Anno 2016, recital 7 of the GDPR states unequivocally that '[n]atural persons should have control of their own personal data'. In the press release on the adoption of the GDPR, rapporteur Jan Philipp Albrecht [11] even emphasised that '[c]itizens will be able to decide for themselves which personal information they want to share'. Behind the scenes, however, his amendment stating that 'the right to the protection of personal data is based on the right of the data subject to exert control over the data that are being processed', was removed from the text agreed upon by the European Parliament [12, 13]. Meanwhile, Article 5(2) provides that the controller shall be responsible for compliance with the data protection principles.

Despite the rhetoric of user control, it will become clear that many provisions in the GDPR serve both the tenet of user control and the tenet of controller responsibility. I will first discuss consent and data subject rights, after which I proceed to the data protection principles, emphasizing their link to the responsibility of the controller.

2.1 Consent and data subject rights

The tenet of user control is guaranteed primarily by the role of consent and the presence of data subject rights in the GDPR and in the ePrivacy Directive. The consent of individuals is a frequently relied-on ground to legitimize the processing of personal data. In many cases, it is the only available legal ground (GDPR, art 9; ePrivacy Directive, arts 6, 9 and 13). The GDPR tightens the definition of consent and strengthens its role. The Data Protection Directive already contained a number of conditions which had to obtain for consent to be valid: consent has to be a 'freely given specific and informed indication of [the data subject's] wishes' (art 2(h)). The GDPR clarifies that consent must always be unambiguous, given either through a statement or a clearly affirmative action (art 4(11), recital 32). The special categories of data, for which consent must be explicit, are expanded (art 8). Further, when assessing whether consent is freely given, 'utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is condi-

tional on consent to the processing of personal data that is not necessary for the performance of that contract' (art 7(4)). Recital 43 clarifies that consent is presumed not to be freely given if the deal is "take it or leave it": if appropriate, consent must be obtained separately for separate processing activities. The provision of a good or service must, in addition, not be made conditional on consent if the consent is not necessary for the performance of the contract. Moreover, the request for consent must be clear. If consent is obtained through a contract or general terms and conditions, the request for consent must stand out, for example by presenting it in a separate text box, and it must be requested in an intelligible and easily accessible form, using clear and plain language (art 7(2)). The information requirements are accompanied by similar demands regarding the form in which they are presented, as necessitated by the principle of transparency (art 12) [14]. In addition to the other information requirements, the data subject must also be informed whether she 'is obliged to provide the personal data' and further 'of the possible consequences of failure to provide such data' (art 13(2)(e)). Finally, if the provision of information society services to children is based on consent, it must have been given or authorized by the holder of parental responsibility over the child (art 9). Purtova [17] argues that developments such as the tightening of the definition of consent have reduced the informational self-determination of the data subject. As a result of these changes, consent will indeed play a smaller role, but it will be more meaningful. Because the conditions under which consent is valid are more stringent, situations under which the data subject did not really make an informed choice will be less readily regarded as an expression of her will.

Individuals are further granted a number of rights, including the right to be informed of a number of categories of information about the processing operation (GDPR, arts 12-14), to access, rectify or erase their personal data (including the "right to be forgotten", arts 15-17), the newfound right to data portability (art 20), and the rights to object and not to be subject to decisions based solely on automated processing (art 21-22). They should be informed of these rights, with the exception, for some reason, of the latter (arts 13(2)(b) and 14(2)(c)). The burden of proof regarding the right to object now unequivocally lies with the controller. If the data subject objects, it is up to the controller to demonstrate 'compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims' (art 21(1)). As befits the level of specificity of an EU regulation, which has direct effect in the legal orders of the Member States, the GDPR now also provides for access to justice and redress, specifying the right to lodge a complaint, the right to an effective remedy, the right to mandate a representative body to lodge a complaint on behalf of the data subject, and the right to compensation (arts 77-80 and 82). These additions serve to provide what Lynskey [13] calls 'an architecture which bolsters individual control', to be distinguished from the control rights themselves. Such an architecture must go beyond the mere provision of information to also include, inter alia, the possibility to take collective action and the availability of actual alternatives in the market. It must be noted, however, that the rights of data subjects do not only serve to grant individuals a certain measure of control. The right to erasure also enables data subjects to ensure that controllers take their responsibility seriously and comply with their obligations, as

they can have their data erased if storage is no longer necessary or if it has become unlawful to keep the data (art 17(1)). The rights to lodge a complaint and to obtain redress can similarly be understood as mechanisms of private enforcement. Further, as discussed in the next section, the rights to be informed and to gain access to the data can also serve to inspire responsible behaviour by shedding "sunlight" on the conduct of controllers.

2.2 The data protection principles and controller responsibility

The tenet of controller responsibility can be found in the data protection principles. It is also strengthened in the GDPR through the addition of a number of novel provisions. The data protection principles of Article 5[1] traditionally sought to establish good governance or due care; requiring that the processing of data is fair and reasonable [3]. Indeed, data protection law can be seen as a substantiation of the overarching principle to process data fairly and lawfully [18, 19], which itself is a reflection of the requirements of good governance or fair administration in the public sector and due care in the private sector under the Dutch tradition [20].

The data protection principles make informational self-determination possible, but they should also spark concern for the interests of data subjects. The principle of lawfulness requires the processing to be based on a legal ground. While consent is one of the legal grounds, a number of other grounds require the controller to gauge the interests of the data subject or of the public at large (GDPR, arts 6(1)(d), 6(1)(e) and 6(1)(f)). The principle of fair processing should also cause the controller to take the interests of data subjects into account. It is frequently understood as requiring that controllers are transparent and do not unduly pressure data subjects into consent, thereby protecting the tenet of user control. However, Bygrave [19] explains that in addition, fairness 'undoubtedly means that data controllers must take account of the interests and reasonable expectations of data subjects', which 'has direct consequences for the purposes for which data may be processed'. This is a form of proportionality, as the interests of data subjects and controllers are balanced [19].

One of the functions of the principle of purpose limitation is to ensure that there are clearly defined processing conditions which can be consented to [21, 22, cf 23]. Data minimization, storage limitation and integrity and confidentiality all require the controller to ensure that these conditions are kept to: that data are not kept longer than necessary or used unnecessarily, and that they are not accidentally processed in unauthorized or unlawful ways. These restrictions should ensure that the processing and its results are legitimate and align to the reasonable expectations of the data subject [19]. This is beneficial for informational self-determination. However, the limitations also serve (or are supposed to serve)[2] as a limit on the processing, preventing the risks

[1] The principles include lawfulness, fairness and transparency; purpose limitation, data minimization and storage limitation; and accuracy, integrity and confidentiality. Purpose limitation entails that the personal data may only be processed insofar as this is necessary for a legitimate and specified purpose.

[2] Moerel and Prins [24] convincingly argue that purpose limitation does not serve as a useful constraint on the processing of personal data when the purpose of controllers is, and is permitted to be, to collect and analyse data.

posed by aimless collection, unlimited dissemination, and misuse or arbitrary use of personal data [25]. Controllers have the responsibility to ensure that the purpose of the processing is legitimate, meaning that they may not process data in ways which do not accord to legal principles, fundamental rights, or other sources of law and that they must take into account the 'reasonable expectations' of the data subject. The Article 29 Working Party [26] mentions by way of example that controllers are prohibited from processing the data 'for purposes that may result in discriminatory practices'. To be clear, this obligation applies irrespective of whether the controller obtained consent from the data subject.

The required transparency towards the data subject clearly makes possible informed consent and the exercise of her rights [14], but also serves to inspire fair and reasonable processing operations: 'sunlight is the best of disinfectants' [15, 16]. It is therefore noteworthy with regard to both tenets of the GDPR that the information requirements are made more specific, requiring controllers to be open about, *inter alia*, their legitimate interest; the storage period; the presence and logic of automated decision-making and the significance and envisaged consequences thereof; and the source of the data, if it had not been provided by the data subject (arts 13(1)(d), 13(2)(a) and (f), and 14(2)(f)). Whereas the Directive only provided a short, non-exhaustive list of the information which should be provided in order for the processing to be fair, the GDPR specifies extensive requirements relating to both the form and the substance of the notices (arts 12-14). These requirements are still to be supplemented under the principles of fairness and transparency, if necessary.

In short, the data protection principles imply that controller responsibility has been, and still is, an important aim of the principles of data protection. A great share of the novelties of the GDPR serve to strengthen the data protection principles. This includes the accountability mechanisms introduced in Chapter IV. Controllers are required to take technical and organisational measures to implement the data protection principles and to protect the rights of data subjects, whereby they have to, by default, limit the processing to what is necessary in accordance with the data protection principles (art 25). Data protection by design should improve compliance with principles such as data minimisation, data quality and confidentiality, as well as ensure that the system is transparent and provides data subjects with effective means of control [7]. Controllers are further obliged under the GDPR to be transparent about data breaches towards both data subjects and supervisory authorities, incentivizing controllers to avoid them in the first place (arts 33 and 34). Moreover, controllers are required to assess and find ways to mitigate high risks to the rights and freedoms of individuals posed by their processing activities (art 35). Recital 75 clarifies that controllers should keep an eye on whether data subjects are able to exercise control over their personal data, but also mentions a large number of other threats and risks, including discrimination, identity theft or fraud, loss of confidentiality of personal data protected by professional secrecy, and unauthorized reversal of encryption. The responsibility to assess and address risks protects data subjects and can function to create a trust relationship between the data subjects and the controller. The two tenets come together here as the controller's responsibility can be indispensable for the data subject's trust

and thus her consent, while this trust relationship also makes the controller responsible to the data subject [27, 28].

Controller responsibility takes place under the supervision of regulatory agencies. The principle of accountability requires controllers to be able to demonstrate compliance (art 24) and to employ and involve a data protection officer (arts 37-39). The GDPR also stimulates the proper translation of data protection law to practice through codes of conduct which can be certified by supervisory authorities (arts 40-43). Although the duty to notify supervisory authorities has been abolished, it has been replaced by the data protection impact assessment and the prior consultation. This should shift the attention of the authorities to potentially harmful cases and enable them to readily gauge the situation at hand (arts 35-36). Article 83 introduces fines up to 20 000 000 EUR or 4 % of the total worldwide annual turnover of an undertaking, whichever is higher.

The second tenet of data protection law should get controllers to provide proper ex ante protection, preventing the occurrence of possible harm to the data subject irrespective of whether she withheld consent or otherwise exercised her control rights. As observed by González Fuster [29], '[r]esponsibility for such compliance had always fallen on their shoulders, irrespective of whether somebody was looking, or whether somebody complains'. In other words, it is the responsibility of the controller to engage in fair practices, although the data subject can have a say in or 'a measure of influence over' what that entails, if she wants to [19].

3 The "choice" to consent and the "paternalism" of protective legislation

The GDPR attempts to strike a balance between the two tenets of user control and controller responsibility. It affords a number of protections irrespective of whether the data subject has consented to the processing. At the same time, consent is an important legal ground for those processing operations which are not easily justifiable on the basis of another ground, e.g. those processing operations which are not necessary to protect the vital interests of the data subject, to perform a task of public interest, or to serve a legitimate interest of the controller which is not outweighed by the rights and interests of the data subjects. Otherwise illegitimate processing operations can only be legitimized through consent. Unsurprisingly, in practice, consent is a weak spot of the GDPR. But what of more protective approaches? The appropriateness of the two tenets depends, firstly, on the significance of the constraints on the free and autonomous choice of data subjects and, secondly, on the permissibility of state intervention for the perceived benefit of the data subject. If data subjects are severely constrained in their choice to consent or not to consent, or are too weak-willed to do what they think is right, there are three options, each of which features in data protection law: their "choice" is still respected; they are protected by default but with the option to opt-out, which may influence their decisions but still allows them, in theory, to "consent away" their rights; or their freedom is curtailed for their protec-

tion. I will first discuss the constraints on choice, after which I will discuss whether the alternative of protection through controller responsibility is paternalist.

3.1 The "choice" to consent

There is extensive literature on the problems with user control, notice-and-consent, privacy self-management, or DIY-data-protection. The majority of the concerns are about constraints on the ability of individuals to freely and autonomously make an informed choice about the data processing operations pertaining to her. Choice always occurs under a set of conditions or parameters [30]. In the words of Cohen [23]: '[s]ome of these parameters, such as the fact that we need gravity to walk and oxygen to breathe, are relatively fixed. Others, such as the design of legal institutions and technological tools, are slightly more malleable'. Benn [31] clarifies that the conditions of choice also relate to states of the agent, distinguishing between the resources which are available to her, the opportunity costs involved in pursuing *X*, the goals of the agent in light of which the choice is made, and the beliefs which the agent holds about these conditions. Restrictions of the freedom of choice can result from restrictions with regard to all four conditions. This means, for example, that the social or economic consequences of refusing to consent and the influence of marketing and online personalization affect the extent to which choice is free. The way in which data protection law regulates consent is bound to legitimize some of these conditions, and change others [32]. It remains to be seen to what extent the changes to the consent regime in the GDPR will make a difference, ameliorating the constraints on the data subject's choice or qualifying consent as invalid because of these constraints. Some data protection scholars think that, in the context of digital services, the restrictions are such that we often can no longer speak of a real choice. If this is so, consent should not be considered informed and freely given.

In the following, the relevant constraints to choice are presented as pertaining to three related categories. Firstly, data subjects do not have enough time to consider each type of processing operation because they engage with services which collect data so very frequently. Or, put differently, they lack the will to make time for this burden — and understandably so, considering how uneconomical it would be [33, 34]. In a well-known study from 2008, McDonald and Cranor 'estimate that reading privacy policies carries costs in time of approximately 201 hours a year, worth about $3,534 annually per American Internet user. Nationally, if Americans were to read online privacy policies word-for-word, we estimate the value of time lost as about $781 billion annually' [35]. While this problem can be addressed by grouping together different types of processing operations, this solution also lumps together different situations in which different values and interests may play a role. It thereby reduces the choice available to data subjects.

Secondly, in the world of "big data", data subjects will often not fully comprehend what it means to consent to a data processing operation. It is difficult, if not impossible, to make data processing operations transparent to the data subjects. Data can be inferred from other available data, so that data which was shared by or inferred about others can be used to infer things about you [33, 36-37]. If complex or self-learning

algorithms are used, the way in which this occurs may not even be explainable in human language [33, 38]. As discussed above, the updated information requirements in the GDPR attempt to increase transparency by requiring controllers to give information on the logic employed by self-learning algorithms, the significance and envisaged consequences thereof, and the other data sources which will be accessed. This information could be presented in accessible and less time-consuming ways, for example through logo's or seals. Doing so, however, 'conflicts with fully informing people about the consequences of giving up data, which are quite complex if explained in sufficient detail to be meaningful' [33]. Or, in the words of Koops [39], 'the simpler you make the consent procedure, the less will users understand what they actually consent to; and the more meaningful you make the consent procedure (providing sufficient information about what will happen with the data), the less convenient the consent will become'.

These first two types of constraints exist irrespective of the actual practices of notice and consent, which oftentimes only make matters worse. Many notices are long and couched in inaccessible language [40], yet fail to shed light on the data flows; they are subject to frequent change; and the privacy policies of those who collect the data are often different from the policies of the entities to which they sell the data [41].

The third type of constraint concerns more or less imposed limitations to the freedom and autonomy of choice. In many situations, data subjects are faced with non-negotiable and excessive "terms", under which personal data can be collected, used and shared almost without limit, while they are unable to get the desired goods or services elsewhere under more reasonable conditions. Underlying this is 'the fact that there are practically no alternative business models that generate revenue from other sources than user-data-based profiling and advertising', given that users are unwilling to pay for services, 'conditioned as they are in thinking that the Internet offers free lunches' (in the words of Koops) [39]. Further, there may well be all kinds of pressures which lead data subjects to desire the product or service. Matzner et al [4] remind us of the costs which are, for many, involved in not owning a smart phone: 'less contacts with friends, missing career opportunities, more complicated dating, being considered inefficient as a colleague, being considered suspicious at border controls'. At the same time, the reasons for using products and services like smart phones and social media 'are promoted by the best advertising agencies in the world'. The situation is grave enough for Hull [32] to imply that the focus on notice and consent in data protection law, rather than decreasing the power dissymmetry, is actually a means to hide and legitimise it. By acting as though the individual has the possibility to exercise real choice, while she in actuality is moulded by the possibilities offered by her (digital) environment, the social struggle is obscured and the individual is disempowered. Cohen [42] also does not mince words, pointing to the power exercised by 'public and private regimes of surveillance and modulation' to turn us into 'citizen-consumers' with diminished capacities of democratic self-government. Cohen [23] suspects that under these conditions of choice, 'individuals may simply concede, and convince themselves that the loss of privacy associated with this particular transaction is not too great'.

Cohen, Solove, Schwartz, Acquisti, and a number of other scholars treat bounded rationality and bias as though they pose cracks through which government and corporate actors manipulate our choices [30, 33-34, 43-44]. Schwartz [30] argues that 'consumers' general inertia toward default terms is a strong and pervasive limitation on free choice' which permits industry to set the terms. Hull [32], on the other hand, sees the notion of *homo economicus* and the resulting reliance on notice and consent in data protection law as the real problem. But if we do not assume that individuals can make autonomous, rational decisions, what is the alternative?

3.2 The "paternalism" of protective legislation

The previous section describes a number of constraints on the ability of data subjects to freely and autonomously form an opinion regarding the appropriateness of certain (aspects of) processing activities, as a result of which they agree to operations which might cause them harm. What conclusion should be drawn from the fact that these constraints exist? Solove [33] believes that 'the most apparent solution — paternalist measures — even more directly denies people the freedom to make consensual choices about their data'. He emphasises that some people want their data shared and want to be profiled, as for them the benefits outweigh the costs. Indeed, proponents of privacy self-management argue that, through a system of user control, 'everyone may attain his own desired level of data protection' [3]. While this is too simple a picture, as there are interdependencies and inequalities — e.g. the data shared by one person can be used to profile another, and some people may be more pressured to share their data than others — [4],[3] control rights do allow an expression of what the data subjects involved consider appropriate in a given situation. Solove sees the EU data protection regime as paternalist because of the many rules which restrict processing even in the absence of any wish or demand on the side of the data subject [33].

To appreciate this point, it is crucial to see that the appropriate limits on data flows and uses of data are not self-evident. Whether a data processing operation is legitimate, entails a normative appraisal of the circumstances at hand. This entails, by way of example, that it is necessary to be sceptical of Cavoukian's attempts to distance her approach to Privacy by Design from paternalism. Cavoukian [45] argues that if controllers implement the fair information practice principles by design, then 'individuals are not placed in the position of having to be concerned about safeguarding personal information — they can be confident that privacy is assured, right from the outset'. She assumes that if controllers simply stick to the principles of purpose limitation and data minimization, the expectations of individuals are respected. The default should be 'the most privacy-protective', and anything extra requires consent [45]. But what is

[3] Matzner et all [4] show that there are inequalities which cannot be addressed on an individual level. Technological means to effectuate control rights are often not free of charge, while, following research of Gilliom, data protection needs are unequally distributed and are likely to hit the poorest. As a result, 'this additional cost is especially put on those who already face discrimination or social inequalities'. Further, there are differences in privacy norms, requiring some individuals to be more revealing than others.

the most privacy-protective default setting? Unlike secrecy, the multi-faceted and contested notion of privacy is not something which can easily be maximized, as it contains conflicting and incommensurable facets which cannot be subsumed under one overarching value without discussion (see section 4.1) [cf 46]. It is difficult to imagine a situation in which secrecy, confidentiality, or even privacy is the only possible consideration, as sometimes data should be shared (see section 4.2).[4] It is therefore problematic to maintain that the implementation of the data protection principles "by design" will protect individuals upfront without the danger of paternalism. The controller will need to consider, for example, whether the purpose is legitimate and whether the impact on data subjects will necessitate extra precautions. Cavoukian's arguments are tempting because we think that it is *right* that certain protections are afforded. The implication is that if we consider something to be of enough moral importance, it should be protected, at least by default, irrespective of what the people concerned actually think about it. This happens to be exactly what paternalism is about.

To start, paternalism can be understood as 'the usurpation of one person's choice of their own good by another person' [47]. While paternalism has a negative connotation, many paternalist measures are accepted on both sides of the Atlantic. To call something paternalist, is only the start of the debate [see e.g. 48]. That said, is the GDPR indeed paternalist, as Solove makes it to be?

Some provisions in data protection law are not only there to protect the data subject, but mainly to empower her or to protect others. Many of the EU rules are necessary preconditions to meaningful consent. Further, some provisions of the GDPR were enacted for the main reason to protect third parties and society as a whole against the harmful or selfish choices which individual data subjects could make in a market-based system of privacy self-management. The legal grounds next to consent and contract all, directly or indirectly, pertain to the interests of others or to the public interest. They allow one's data to be used for the benefit of others. Other provisions limit the use of data, possibly to address societal problems posed by function creep. It has been argued that the problems which should be addressed by data protection law, pertain to the interests of society as a whole; because everyone is or might be a data subject, it is no longer about protecting specific individuals [3]. Privacy is seen as a 'common good' [43]. Insofar as the provisions of the GDPR were not included to protect the individual whose choice is usurped, they do not qualify as paternalist [49].

[4] It is possible to hold that secrecy or confidentiality *should be* the only mandatory consideration when technology is designed, as appears to be the case under the Privacy by Design requirement in the proposed ePrivacy Regulation. Article 10 of the leaked Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and personal data in electronic communications and repealing Directive 2002/58/EC requires that the default setting of terminal equipment and of software should be that third parties can neither store information on the equipment, nor process information which is stored thereon. Internet browsers, for example, should automatically reject all third-party cookies. The end-user can consent to these processing activities of third parties by changing the browser settings per Article 9(2) — assuming that this option is provided by the developers of the browser.

At the same time, however, a concern for the interests of the specific data subject and the risks or possible consequences for this data subject is present throughout the GDPR. The data subject cannot "consent away" the protection offered to her by the principles of fairness, purpose limitation, data minimization, data quality and data security, and this is in part for the protection of her own rights and freedoms. The GDPR thus includes paternalist provisions.

Sometimes, the data subject can opt out of the protection which is offered, as when she can opt in to more extensive processing as per data protection by default. Under some definitions of paternalism, such as that of Thaler and Sunstein [50] and of Dworkin in his later work [51], the fact that a user can, at least in theory, opt out of the paternalist measure, does not mean that the intervention is not in fact paternalist. Any nudge, including a change in the default setting, is considered paternalist if it is for the agent's own good. This is because the choice or decision-making of the agent is influenced [50-52]. Her choice is not necessarily usurped, but it is certainly affected. Since the nudge only seeks to prevent actions that stem from irrational tendencies, which assumedly should be kept in check by one's rational, 'Econ' side [53], it bears resemblance to Feinberg's [54] 'soft paternalism'. However, paternalism can also be understood as entailing that the agent's freedom is curtailed. The paternalism of a nudge then depends on whether or not the agent truly has the option to opt out. Because the default setting is often followed, it could be argued that a change in the default affects the options available to the agent. It thus limits her freedom, albeit the freedom to be irrational, as well as her autonomy [cf 55].

The GDPR thus seeks to protect data subjects, although they can sometimes opt out of this protection. What if this is what they want? In theory, the protections which are afforded could be in accordance with what the data subject would want and possibly even with what she would choose, if she had the time, the knowledge and the capacity to fully reflect on it [cf 'anticipated consent', 56]. This appears to be Cavoukian's answer to the charge of paternalism. However, it is unlikely that a general set of rules will meet the anticipated wishes of every data subject, as they are bound to differ. Moreover, even if people value their privacy, many do find themselves giving away their data. This is the so-called "privacy paradox". Following Shiffrin [57], protecting people from the privacy paradox would count as paternalism. Shiffrin discusses the case in which the friend of a smoker hides her cigarettes because, even though she wants to stop smoking, she might be weak-willed and light another cigarette. Such an intervention should be considered to be paternalist because 'efforts to supplant or maneuver around an agent's agency when motivated by distrust of that person's agency, can deliver the same sort of insult to her autonomy as distrust of her judgment'. Archard [47] takes a different approach. According to Archard, it is necessary that the paternalist discounts the agent's belief that his intervention does not promote her own good, and so there must be disagreement about the benefit of the intervention.

Would the protection afforded by the GDPR be paternalist if the data subject has not formed a conscious choice? Users are bound to accept cookies and download apps without fully considering the data protection consequences (see section 3.1). In that case, protective legislation would restrict the freedom of the data subject, but it would not necessarily impinge her autonomy, as the data subject is not giving expression to a

full-fledged decision. Her choice is not necessarily usurped, as she did not really make a choice, but the option to act differently has been taken from her**.** Clarke [58] considers cases in which a choice is made for someone who was unable to make the choice herself, to be paternalist. In his example, an unconscious patient is given a blood transfusion. The incapacity to reflect on each exchange of personal data in today's information society could be considered to similarly affect whether a data subject has the ability to choose, albeit to a lesser extent. It is important to note that while a choice can be formed more or less reflectively or deliberately, meaning that factual autonomy is gradual, a person is often morally and legally granted the freedom of 'a valid decision-making body' if she meets a certain threshold of rationality, self-reflection and self-control [31, 59]. Consumer law, for example, sees consumers as reasonably well-informed, observant and circumspect, which strikes a particular 'balance between the need to protect consumers and promoting free trade' [14]. While it is now popular in data protection scholarship to 'question the very possibility of [user] control by deconstructing the conventional figure of the "rational and autonomous agent" that is at the core of "privacy as control" theories' [43], only a limited "amount" of rationality and autonomy is needed to sustain the tenet of user control in data protection law. The legal question is whether the average data subject, who could not take the time to find and read an incomprehensible privacy policy and who was nudged by her digital environment and socio-economic context to click on 'OK' in favour of short-term gain, should qualify as autonomously and freely making an informed choice. And if the answer is no — if we assume that data subjects cannot make autonomous, rational decisions in the online context — the follow-up question is whether this means that her freedom can be restricted, or whether her "choice" should be respected nonetheless.

4 How to evaluate the tenets of user control and controller responsibility

It follows from the analysis in section 2 that the GDPR places heavy reliance on enforcement by both private and supervisory authorities so as to ensure that controllers process data fairly — both to enable data subjects to exercise their control rights and to prevent controllers from bringing about unjustifiable harm. The GDPR seeks to *empower* and to *protect*. But how to interpret and apply these tenets? On the basis of which benchmarks do we decide whether to foster choice and accept indications of consent, despite the constraints discussed, or to opt for more protective, even paternalist, approaches instead? Evaluations of user control are fraught with conceptual difficulty. As remarked by Lazaro and Le Métayer [43], it is important to distinguish between user control as part of the foundation of data protection and user control as nothing but private enforcement. Private enforcement options may have been introduced to overcome the failing of a purely administrative set of rules, but they also restore, in the words of Purtova [3], 'the balance of power between individuals and data processing actors'. In the evaluation of Bygrave and Schartum [60], data protection law is about protecting privacy and data protection interests, whereby consent

should ‘strengthen the bargaining position of individuals’. In the next sections, I will argue that the aim of data protection can be to protect specific interests but also to empower, depending on how the objective of the GDPR to protect fundamental rights is conceptualized. Under a will theory of rights, user control is indispensable, despite the constraining conditions of choice, while an interest theory of rights supports a large role for controller responsibility, despite the paternalism of this tenet.

4.1 User control or controller responsibility — to what end?

Whether private enforcement is a welcome addition or whether it is essential to the goal of data protection, depends on how the foundation and objective of data protection is conceptualized (and in particular, as will be argued in section 4.3, on how rights are conceptualized). I will discuss the protection of interests of the data subjects, including the interest in being granted ‘a zone of relative insulation from outside scrutiny and interference’ [23], and informational self-determination: an empowering objective which is frequently seen as the justification for the tenet of user control.

If the focus is on a protective goal of the GDPR, it is easy to conclude that data protection law is the responsibility of controllers, meaning that protective rules are an appropriate response to the constraints on the ability of data subjects to exercise choice. When Matzner et al [4] argued that it is not normatively desirable ‘to choose the individual user as the main responsible actor to improve the state of data protection’, they saw data protection as is something which citizens ‘need’. They asked whether it should be up to data subjects to ensure that their data is protected in the sense that ‘particular pieces of data should not be accessible to particular actors’. Since they have identified an interest which deserves protection, they can see data protection as something which needs to be protected by controllers and by the state for the benefit of data subjects. The GDPR protects a wide range of interests of individuals or society in general in relation to the processing of personal data. It protects not only confidentiality and data security, but also the right not to be discriminated and the right not to be unduly subjected to a profile. The GDPR takes on board all these different harms, seeking to ensure that the controller takes the interests of data subjects into account and abstains from taking unjustifiable risks. Interestingly, it also asks for particular attention ‘where personal data of vulnerable natural persons, in particular of children, are processed’ (recital 75).

One privacy interest which can be protected by controllers, is the interest in having a space to develop one’s identity without undue outside interference. Multiple theories of privacy view this right as granting individuals a private zone within which they can consciously and with relative autonomy engage in self-formation [42, 61]. For Cohen, privacy in this sense is severely affected by profiling. The practice of profiling can make data flows less transparent and predictable [22], and it can lead to harmful and unjust decisions. However, privacy scholars like Cohen [23] are particularly concerned about the impact of the use of profiles for online personalisation on an individual’s ability to autonomously construct her identity. The nudging effect of digital environments complicates autonomous user control and creates an interest which can be protected. To ask data subjects to ensure that they are not subject to undue modula-

tion and interdiction, defeats the purpose. If it is done well, they will not be aware of the effect; they will perceive their preferences and actions as authentic. They may even offer their consent in the future [23, 32]. Thus, if certain interferences with an individual's process of self-formation simply should not be undertaken, then it is primarily the responsibility of controllers to refrain from adopting such illegitimate purposes. In the typology of Koops et al [62], seclusion, secrecy, and control lie on a continuum of accessibility from private to public. While this may be so, the former two require protection, and the latter requires empowerment.

User control necessarily plays a prominent role in data protection if the focus is on the right to informational self-determination and on the power available to individuals to push back and to engage in 'boundary management' [42]. It was of great influence to the EU data protection tradition that the German *Bundesverfassungsgericht* brought to life the right to informational self-determination in 1983 [63]. This right is defined as follows: 'the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others' [21-22, 64]. Underlying this right is a concern about chilling effects. If you cannot predict which information is known about you in certain 'social milieus', then your decisions will be subject to 'pressure influence' [21]. For example, the *Bundesverfassungsgericht* [21] argued that '[i]f he [the individual] reckons that participation in an assembly or a citizens' initiative will be registered officially and that personal risks might result from it, he may possibly renounce the exercise of his respective rights'. More generally, as noted by Hornung and Schnabel [22], '[i]f citizens cannot oversee and control which or even what kind of information about them is openly accessible in their social environment, and if they cannot even appraise the knowledge of possible communication partners, they may be inhibited in making use of their freedom'. The court [21] ties this to the German constitutional right to personality, arguing that chilling effects impair an individual in her chances of self-development and thereby stand in the way of a free democratic society.

Taking a cue from Purtova's [3] view of data protection law as restoring the power balance between data subjects and controllers, and from the focus of the *Bundesverfassungsgericht* [21] on chilling effects to fundamental rights, I propose that informational self-determination protects political power. It protects the influence which an individual or group of individuals can have over what it means to hold fundamental rights in a given polity. This is because it limits the extent to which other actors in society, be they governmental or private, can preclude certain activities. For example, if the state is aware of the meetings of a controversial political group, it is in the position to prohibit the assembly, thereby determining that it is not worthy of protection under the relevant rights and freedoms. Similarly, an individual may wish to hide sensitive information about herself in specific contexts so as to prevent others from discriminating her on the basis of that information — thereby protecting her right to equal treatment, as she perceives it. Her ability to control whether the sensitive information is known, allows her to act on her belief that the information should be irrelevant to others: that it is private in the sense that it is *just* for her to hide it. Informational self-determination therefore indirectly safeguards the ability of individuals to

define, for themselves, what their interests and needs are and how they should be protected in a just society. For example, the right to object allows data subjects to object to processing which takes place on the basis of the public interest or a legitimate interest of the controller or of a third party (GDPR, art 21(1)). This means that, if a data subject does not agree with the balance between this other interest and her own rights, the right to object provides an avenue through which she can make herself heard.

The *Bundesverfassungsgericht* considered it crucial that individuals have control over information flows for the protection of other rights and freedoms, to the extent that control was deemed to be a right of its own. Informational self-determination protects an interest or need, but it is different from other interests as it is now essential that the data subject takes an active role. The state may need to require controllers to amend their conduct in order to establish a situation in which effective control is possible. If control rights are unenforceable because of the complexity of the Big Data landscape [39], the right to informational self-determination would demand state intervention to remedy the situation.

It is important to note that the right to informational self-determination is not absolute. Thus it is possible that certain information flows should or should not occur, irrespective of the wishes of the data subject. Depending on the political theory of choice, it could be desirable to limit the use of profiles so as to protect the relatively autonomous self-formation of individuals, or perhaps profiles should be used to create a public space where political deliberation occurs, or, alternatively, to offer the safety promised by the Hobbesian state [cf 65]. In the German tradition, informational self-determination is only the 'intermediate value' adopted by the *Bundesverfassungsgericht* to protect the higher rights to dignity and personality [63]. Rouvroy and Poullet [63] argue, in this vein, that the two facets of privacy tied to seclusion and control ultimately do not pursue different goals, as they together sustain self-determination and collective decision-making. Both the right to be let alone so as to engage in relatively autonomous self-formation, and the right to informational self-determination, advance 'the capacity of the human subject to keep and develop his personality in a manner that allows him to fully participate in society without however being induced to conform his thoughts, beliefs, behaviours and preferences to those thoughts, beliefs, behaviours and preferences held by the majority'. Undeniably, however, the two tenets do come into tension. When an individual is or is not granted privacy against her wishes, she has little say over what the right to privacy means or should mean. Her capacity to develop thoughts, beliefs, behaviours and preferences may be protected, but her power to affect what the right to privacy should entail is diminished for the sake of developing this capacity, limiting the control she has over the boundary between her and others.

4.2 Fundamental rights protection as the overarching objective of the General Data Protection Regulation

To evaluate the roles for user control and controller responsibility, given the issues these tenets face with choice and paternalism, it is necessary to look beyond either

informational self-determination or another interest or need which can be protected. How do we get past stand-offs in which scholars emphasize one side or the other? While the *Bundesverfassungsgericht* can appeal to the higher right to personality, the EU legal order lacks an equivalent. In the absence of a similar over-arching right, this paper proposes to ask the question of responsibility with an eye to fundamental rights in general.

From a doctrinal perspective, the objective of the GDPR to protect fundamental rights overarches the different tenets of data protection. The question of responsibility thus becomes an inquiry into what it means to protect or enjoy fundamental rights. In accordance with Article 1, the GDPR protects the fundamental rights and freedoms of natural persons and *in particular* their right to the protection of personal data with regard to the processing of personal data. The GDPR no longer protects, in particular, the right to privacy, as did the Data Protection Directive. The right to the protection of personal data, laid down in Article 8 of the Charter, has taken this place. Article 8(2) elevates the status of a number of data protection principles, which were designed to regulate the processing of personal data in a manner which achieves an appropriate balance between the different rights and interests involved. The processing of personal data has a bearing on many different fundamental rights. When the EU legislature decided to further substantiate the meaning of the right to the protection of personal data by adopting the GDPR, it remained fully aware that not one right could take priority in the resulting legal framework [e.g. 66]. This is made evident by the frequent reference to "the rights and freedoms of individuals" throughout the GDPR, which must, according to the Article 29 Working Party [67], be understood as referring to not only privacy, but also to 'other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion'. Importantly, recital 4 reminds us that the right to the protection of personal data is not an absolute right, and that it must accordingly be balanced against other fundamental rights so as to respect them, too. It thus states that the GDPR respects all fundamental rights, mentioning explicitly 'the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.' The Commission's draft General Data Protection Regulation [10] similarly enumerated a number of relevant rights, including further the right to property, the prohibition of discrimination, the rights of the child, the right to health care, and the right to access documents.

The free flow of personal data is a particularly important consideration in EU data protection law. Article 1 GDPR refers to the fundamental freedoms of the internal market and provides that the free flow of personal data shall neither be restricted nor prohibited to protect fundamental rights. This is a remnant of the focus of the EU on the establishment of an internal market. In the area of data protection law, fundamental rights protection is articulated and offered by the EU partly because differences in the level of protection would affect the free flow of information (recital 9) [10]. This rationale must, however, not be overestimated. The CJEU pays less and less attention to the internal market dimension [13, 68]. Although the EU can still be characterized

as a separate legal order by virtue of its pursuit of 'the market-driven integration of nation states into a supra-national entity', it also 'increasingly commits itself to the political project of protecting fundamental rights' [69]. Lynskey [13] points to Article 16 TFEU as freeing data protection law from its internal market constraints. She also highlights the contentious nature of this second, economic, ambition of the GDPR. The free flow of information is no longer the main aim of EU data protection law, but it can be one of the considerations which needs to be taken on board when the balance between the relevant rights and other considerations is struck.

The turn of data protection law away from the internal market and away from privacy alone, towards fundamental rights in general, ties in well with modern privacy and data protection scholarship. The recognition of other rights and freedoms is present in Nissenbaum's [70] theory of privacy, as some data flows are appropriate and others are not. The appropriateness of data flows is not at all dependent solely on the amount of secrecy or control which is provided. The processing of certain types of information can be deemed inappropriate because, amongst other reasons, it may lead to restrictions of other fundamental rights. Rouvroy and Poullet [63] observe that 'data protection is also a tool for protecting other rights than the right to privacy', as data protection law also prevents potential discrimination given the regime for special categories of data.[5] Some data protection scholars [71-74] consider data protection a purely procedural body of law which serves other rights and freedoms. It 'does not directly represent any value or interest per se, it prescribes the procedures and methods for pursuing the respect of values embodied in other rights' [71]. In the words of De Hert and Gutwirth [74], data protection law provides channels for the coordination of different rights and competing considerations, through which controllers should 'reconcile fundamental but conflicting values such as privacy, free flow of information, the need for government surveillance, applying taxes, etc'.[6]

4.3 The nature of (fundamental) rights

It is not only doctrinally appropriate, it is also illuminating to assess the appropriate roles of user control and controller responsibility with reference to the nature of fundamental rights. This perspective opens up the discussion on whether or when it is appropriate for the GDPR to empower or to protect. At first sight, it makes sense to encumber the controller and state institutions with the protection of fundamental rights. The state is under both negative and positive obligations to respect and protect fundamental rights. Respect for fundamental rights makes a legal order legitimate. The required action or abstention does not need to be claimed by the rights-holder. However, the matter of rights becomes more complicated if one recognizes that the substance of fundamental rights is not a given. It is determined by the polity in which

[6] A difficulty is that the protection of personal data is conceptualised differently in the different Member States. Gellert, De Hert and Gutwirth have developed their view on EU data protection from a Belgian background, and according to González Fuster [64], Belgium is one of the Member States 'where the protection of personal data is conceived as primarily serving other existing rights'.

they apply, and it is subject to intense contestation. As noted by Waldron [75], '[a]ny theory of rights will face disagreements about the interests it identifies as rights, and the terms in which it identifies them. Those disagreements will in turn be vehicles for controversies about the proper balance to be struck between some individual interest and some countervailing social considerations' [69]. This gives the concern over paternalism in data protection law a particular sting, as it affects not only the forms of freedom and autonomy which an individual can legitimately enjoy, but also, in particular, her say regarding the substance of fundamental rights protection in her polity. In other words, it affects her say on what justice entails and on when authority is legitimate.

The answer to the question of responsibility depends on whether a will-based theory or an interest-based theory of rights is adopted. Interest theories see it as the function of rights to promote the interest or well-being of the rights-holder by giving her the benefit of another's duty. The idea is that some interests merit special attention. A right exists because there is an interest which requires protection [76]. One's right is a legal, possibly a fundamental, right 'if it is recognized by law, that is, if the law holds his interest to be sufficient ground to hold another to be subject to a duty' [77]. The rights-holder is protected for her benefit, as under many of the provisions of the GDPR. The fact that rights are respected "by default" and cannot be waived, entails that individuals who lack the freedom, autonomy or agency to adequately claim and defend their rights, are protected. However, this raises the question whether the interest-based approach should be taken on, particularly in the legal context, as rights are granted or withheld on the basis of another's perception of the rights-holder's interests (at best) [77]. If someone is perceived as having an interest, and accordingly is granted a right which the duty-holder respects, while the person concerned would not agree to this state of affairs, her choice is usurped for her own good. Thus, interest-based rights promise us the same double-edged sword as controller responsibility. Data subjects are afforded the protection of the principles of fairness, purpose limitation, data minimization, etcetera, even if they cannot adequately make use of their legal powers to choose what to consent to and to object to a processing operation. However, they are afforded this protection whether they want it or not. As under an interest theory of rights, data subjects are denied the political power to fully determine what the protection of their rights should look like. It is therefore interesting for the evaluation of controller responsibility to see how interest theories tackle the charge of paternalism.

If the tenet of controller responsibility shares the problems of an interest theory of rights, the correlate of the tenet of user control is a will theory of rights. Will theories see the function of rights not as the protection of one's interests (unless perhaps the interest is that of autonomy [78]), but as granting the rights-holder control over the duty of another [79]. The purpose and value of rights is precisely that it grants authority and permits the exercise of choice. The rights-holder can waive, annul or transfer the duties of the duty-bearer; the right is at her disposition. 'To have a right is to have the ability to determine what others may and may not do, and so to exercise authority over a certain domain of affairs' [80]. This is akin to how the right to privacy is often used in common parlance: as a shield which allows an individual to exclude others

from a certain sphere within which she should have full sovereignty. It is also akin to the notion of informational self-determination, which grants the rights-holder control over whether others may access her information and over what they may do with this information. The options to withhold or withdraw consent, to opt-in to more extensive processing operations, to correct your data, and to object, grant a measure of control over the conduct of others. Again, though, this theory offers a double-edged sword. A challenge for will theory is that it 'could (...) be used, at least in principle, to justify slavery or absolute subjugation, since people could be thought of as having sold or abdicated their liberty, for the price of subsistence or security, to a master or a king' [81]. Will theory leaves those who are not able to demand their rights in line with their interests, without protection. The role of consent in data protection law similarly exposes data subjects who do not act in accordance with their interests when they agree to a data processing operation. Without additional protection, data subjects would be able to "consent away" their privacy, irrespective of the conditions under which this choice occurs. In the extreme, will theory leaves incompetent or non-autonomous individuals without any protection, as they do not even qualify as a rights-holder. This forces the will theorist to resort to proxies that can exercise power for them, such as parents or legal guardians [78]. One of the challenges for will theorists is whether rights apply to all those who can express a preference (in the worst case, like a mollusc '"chooses" to close its shell to avoid intruders and to open it to admit nourishment [78]), or only to those who have made a conscious, autonomous choice — and where to draw the line. In the GDPR the line is drawn at the age of 16, as children are unable to give consent without the authorisation of the holder of parental responsibility (art 8(1)). It is relevant for the role of user control to assess how and why will theorists justify the alienability of rights and the reliance on proxies. Should data protection law follow their cue, if it is to take its aim to protect fundamental rights seriously, and if not, why not?

5 Conclusion

Asking whether data protection is the responsibility of the state, this paper has explored the presence of user control and controller responsibility in the GDPR and paved the way for an in-depth evaluation of these two tenets in light of the overarching objective of the GDPR to protect fundamental rights. The paper brings to the fore a dilemma which is present in the debate on "notice-and-consent" and which ties in well with the debate between will-based and interest-based theories of rights. If one has in mind a set of pre-defined interests, such as the interest in seclusion or the interest in secrecy, it is not problematic to conclude that the GDPR should require controllers to protect data subjects. In practice, however, the appropriateness of data flows is not clear-cut. When data processing operations are restricted for the benefit of data subjects, certain rights, interests or other considerations are accorded greater weight than others even though data subjects themselves may disagree. User control is important because it gives data subjects the political power to assert whether they think specific data flows are appropriate. Control rights allow them to decide on the appro-

priateness of the data processing operations which affect them in light of the balance between the applicable rights and interests which they think should be struck. Thus, there is something to be said for placing the responsibility for data protection primarily with data subjects. This enlarges their power to partake in the formulation of the meaning of fundamental rights in specific situations. Then again, the constraints on the ability of a data subject to freely and autonomously exercise her control rights might lead her to inadequately defend her interests. We need to consider the conditions under which choice is or is not respected: the information which is presented, and how it is conveyed; the availability and popularity of other options in the market; the digital environment within which data is collected and used; and the overall socio-economic context, influencing not only what is possible for the data subject in the given architecture or code, but also her goals and desires, and how her options, goals and desires are perceived [3, 13, 63]. The more constraining the conditions of choice, the more attractive the protective track of controller responsibility. If we truly do not regard the data subject's choice as free and autonomous, this may entail that her freedom should be restricted so as to offer protection. Perhaps, then, it is better for the GDPR to offer protection with the perceived interests of data subjects and society as a whole in mind.

How to assess which edge of the double-edged sword to sway; user control, or controller responsibility? Under the GDPR, the benchmark is that of the protection of the fundamental rights and freedoms of individuals. The question of responsibility thus becomes whether the protection of the fundamental rights of data subjects is something which controllers, under the supervision of supervisory authorities, should take on for the benefit of the individuals concerned. This perspective allows the dilemma to be further analysed and evaluated in light of will-based and interest-based theories of rights. How do these theories justify the shortcomings of an approach which protects the perceived interests of individuals, and those of an approach which vests authority in the individual? Presumably, if, on the one hand, the rights of data subjects serve to protect their interests, the bullet of paternalism has to be bit; on the other hand, if their rights assume a great deal of moral and political capacity and thereby require them to engage in an active expression of their preferences or choices, any further protection cannot occur in the name of fundamental rights.

References

1. Zuiderveen Borgesius, F.J.: Improving privacy protection in the area of behavioural targeting. PhD thesis, University of Amsterdam, Amsterdam (2014)
2. van der Sloot, B.: Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. International Data Privacy Law 4, 307-324 (2014)
3. Purtova, N.N.: Property rights in personal data: A European perspective. BOXPress BV, Oisterwijk (2011)
4. Matzner, T., Masur, P.K., Ochs, C., von Pape, T.: Do-It-Yourself Data Protection – Empowerment or Burden? In: Gutwirth, S., Leenes, R., De Hert, P. (eds): Data Protection on

the Move. Current Developments in ICT and Privacy/Data Protection (Law, Governance and Technology Series, vol. 24). pp. 277-305. Springer, Dordrecht (2016)
5. O'Mailey,P.: Responsibilization. In: Wakefield, A., Fleming, J. (eds): The SAGE Dictionary of Policing. SAGE, London (2009)
6. European Commission: Communication on personal data protection in the European Union. COM(2010) 609 final
7. Article 29 Data Protection Working Party, Working Party on Police and Justice: 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 (2009)
8. Article 29 Data Protection Working Party: Opinion 3/2010 on the principle of accountability. WP 173 (2010)
9. European Commission: Impact Assessment accompanying the General Data Protection Regulation. SEC(2012) 72 final
10. European Commission: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM (2012) 11 final
11. European Parliament, http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era
12. Parltrack Jan Philipp Albrecht, 2012/0011 (COD) Personal data protection: processing and free movement of data (General Data Protection Regulation), 2013/01/16 LIBE, Amendment 29 #http://parltrack.euwiki.org/mep/ALBRECHT%20Jan%20Philipp
13. Lynskey, O.: The Foundations of EU Data Protection Law. Oxford University Press, Oxford (2015)
14. González Fuster, G.: How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection. Revista de Internet, Derecho y Politica 19, 92-104 (2014)
15. Koops, B.J.: On decision transparency, or how to enhance data protection after the computational turn. In: Hildebrandt, M., De Vries, K.: Privacy, Due Process and the Computational Turn. pp 196-220. Routledge, Abingdon (2013)
16. Moerel, E.M.L.: Big data protection: How to make the draft EU Regulation on Data Protection Future Proof. Inaugural lecture, Tilburg University, Tilburg (2014)
17. Purtova, N.N.: Default entitlements in personal data in the proposed regulation: informational self-determination off the table ... and back on again?. Computer Law and Security Review 30(1), 6-24 (2013)
18. Bainbridge, D.: Introduction to Computer Law. Pearson Longman, Harlow (2004)
19. Bygrave, L.A.: Data Privacy Law. Oxford University Press, Oxford (2014)
20. *Kamerstukken II* 1997/98, 25892, 3
21. BVerfGE 65, 1 – *Volkszählung*
22. Hornung, G., Schnabel, C.: Data protection in Germany I: The population census decision ad the right to informational self-determination. Computer Law & Security Report 25(1), 84-88 (2009)
23. Cohen, J.E.: Examined Lives: Informational Privacy and the Subject as Object. Stanford Law Review 52(5) Symposium: Cyberspace and Privacy: A New Legal Paradigm? 1373-1438, (2000)
24. Moerel, L., Corien, P.: Privacy voor de homo digitalis: Proeve van een nieuw toetsingskader voor gegevensbescherming in het licht van Big Data en Internet of Things. Homo Digi-

talis. Preadviezen 2016 Nederlandse Juristen-Vereniging, pp 9-124. Kluwer Juridisch, Deventer (2016)
25. Brouwer, E.: Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation. In: Besselink, L., Pennings, F., Prechal, S. (eds): The Eclipse of the Legality Principle in the European Union. pp. 373-295. Kluwer Law International, Alphen aan den Rijn (2011)
26. Article 29 Data Protection Working Party: Opinion 03/2013 on purpose limitation. WP 203 (2013)
27. Nickel, P.: Consent and uncertainty in biobanking and biomedical data (forthcoming)
28. Pellizzoni, L.: Responsibility and Environmental Governance. Responsibility and Environmental Governance, Environmental Politics (13)3, 541-565 (2004)
29. González Fuster, G.: Beyond the GDPR, above the GDPR. In: Internet Policy Review. 30 November 2015, http://policyreview.info/articles/news/beyond-gdpr-above-gdpr/385
30. Schwartz, P.M.: Internet Privacy and the State. Conn L Rev 32, 815-859 (1999)
31. Benn, S.I.: Freedom, Autonomy and the Concept of a Person. Proceedings of the Aristotelian Society, New Series, vol. 76, 109-130 (1975-1976)
32. Hull, G.: Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. Ethics and Information Technology 17(2), 89-101 (2015)
33. Solove, D.: Introduction Privacy self-management and the consent dilemma. Harvard Law Review 126, 1880-1903 (2013)
34. Van Alsenoy, B., Kosta, E., Dumortier, J.: Privacy notices versus informational self-determination: Minding the gap. International Review of Law, Computers & Technology 28, 185-20 (2014)
35. McDonald, A.M., Cranor, L.F.: The Cost of Reading Privacy Policies. A Journal of Law and Policy for the Information Society I/S 4(3), 540-565 (2008) 4(3)
36. Hildebrandt, M.: Who is Profiling Who? Invisible Visibility. In: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds): Reinventing data protection? pp . 239-253 Springer, Dordrecht (2009)
37. Le Métayer, D., Le Clainche, J.: From the Protection of Data to the Protection of Individuals: Extending the Application of Non-discrimination Principles. In: Gutwirth, S., Leenes, R., De Hert, P., Poullet, S. (eds): European Data Protection: In Good Health? pp. 315-331 Springer, Dordrecht (2012)
38. Zarsky, T.: Transparent Predictions. University of Illinois Law Review 4, 1503-1570 (2013)
39. Koops, B.J.: The trouble with European data protection law. International Data Privacy Law (2014)
40. Article 29 Data Protection Working Party: Opinion 10/2004 on More Harmonised Information Provisions. WP 100 (2004)
41. Barocas, S., Nissenbaum, H.: On Notice: The Trouble with Notice and Consent. Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information. Cambridge (2009)
42. Cohen, J.E.: What Privacy is For. Harvard Law Review 126, 1904-1933 (2012-2013)
43. Lazaro, C., Le Métayer, D.: Control over personal data: true remedy or fairytale? SCRIPTed 12(1), 3-34 (2015)
44. Cohen, J.E.: Between Truth and Power. In: Hildebrandt, M., van den Berg, B. (eds): Freedom and Property of Information: The Philosophy of Law Meets the Philosophy of Technology. Routledge (forthcoming), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2346459

45. Cavoukian, A., Dix, A., El Emam, K.: The Unintended Consequences of Privacy Paternalism. Information and Privacy Commissioner, Ontario, 5 March 2014
46. van de Poel, I.: Translating Values into Design Requirements. In: Michelfelder, D.P. et al 9eds); Philosophy and Engineering: Reflections on Practice, Principles and Process. Philosophy of Engineering and Technology, vol. 15, pp. 253-266. Springer, Dordrecht (2013)
47. Archard, D.: Paternalism Defined. Analysis 50(1) 36-42 (1990)
48. Conly, S.: Against Autonomy. Justifying Coercive Paternalism. Cambridge University Press, Cambridge (2013)
49. Bullock, E.: A normatively neutral definition of paternalism. The Philosophical Quarterly 65, 1-21 (2015)
50. Thaler, R.H., Sunstein, C.R.: Libertarian Paternalism. American Economic Review 93(2), 175-179 (2003)
51. Dworkin, G.: The Theory and Practice of Autonomy. Cambridge University Press, Cambridge (1988)
52. Dworkin, G.: Defining Paternalism. In: Schramme, T. (ed): New Perspectives on Paternalism and Health Care. Springer International Publishing (2015)
53. Hansen, P.G.: The definition of Nudge and Libertarian Paternalism: Does the Hand Fit the Glove? EJRR 1, 155-174 (2016)
54. Feinberg, J.: Harm to Self. The Moral Limits of the Criminal Law. Oxford University Press, Oxford (1986)
55. Bernal, P.: Internet Privacy Rights. Rights to Protect Autonomy. Cambridge University Press, Cambridge (2014)
56. Kleinig, J.: Paternalism. Manchester University Press, Manchester (1983)
57. Shiffrin, S.V.: Paternalism, Unconscionability Doctrine, and Accomodation. Philosophy & Public Affairs 29(3) 205-250 (2000)
58. Clarke, S.: A definition of paternalism. Critical Review of International Social and Political Philosophy 5(1), 81-91 (2002)
59. Fateh-Moghadam, B., Gutmann, T.: Governing [through] Autonomy. The Moral and Legal Limits of "Soft Paternalism". Ethical Theory Moral Practice 17, 383-397 (2014)
60. Bygrave, L.A., Schartum, D.W.: Consent, Proportionality and Collective Power. In: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds) Reinventing Data Protection? Springer, Dordrecht (2009)
61. Richards, N.M.: Intellectual Privacy. Texas Law Review 87, 387-445 (2008)
62. Koops, B-J et al: A Typology of Privacy. University of Pennsylvania Journal of International Law 38(2) (2016)
63. Rouvroy, A., Poullet, Y.: The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy. In: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds): Reinventing data protection? pp 45-76. Springer, Dordrecht (2009)
64. González Fuster, G.: The emergence of personal data protection as a fundamental right of the EU. Springer, Cham (2014)
65. van der Sloot, B.: Privacy as a tactic of norm evasion, or why the question as to the value of privacy is fruitless. In: Janssens, L.: The Art of Ethics in the Information Society. Amsterdam University Press, Amsterdam (2016)
66. Joined cases C-92/09 and C-93/09 Volker und Markus Schecke [2010] ECR I-11063
67. Article 29 Data Protection Working Party: Statement on the role of a risk-based approach in data protection legal frameworks. WP218 (2014)

68. Irion, K.: A special regard: The Court of Justice and the fundamental rights to privacy and data protection. In: Faber et al (eds): Festschrift für Wolfhard Kohte. Nomos, Baden-Baden (forthcoming)
69. Augenstein, D.H.: Disagreement – Commonality – Autonomy: EU Fundamental Rights in the Internal Market. Cambridge Yearbook of European Legal Studies. 15, 1-26 (2013)
70. Nissenbaum, H.: Privacy as contextual integrity. Washington Law Review 79, 119-158 (2004)
71. de Andrade, N.: Oblivion: the right to be different.. from oneself. Reproposing the right to be forgotten. Revista de los Estudios de Derecho y Ciencia Política de la UOC 13, 122-137 (2012)
72. Zanfir, G: Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law. In: Gutwirth, S., Leenes, R., De Hert, P. (eds): Reloading data protection: multidisciplinary insights and contemporary challenges. pp. 327-259. Springer, Dordrecht (2014)
73. Gellert, R., Gutwirth, S.: The legal construction of privacy and data protection. Computer Law & Security Review 29, 522-530 (2013)
74. De Hert, P., Gutwirth, S.: Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds): Reinventing data protection? pp. 3-44. Springer, Dordrecht (2009)
75. Waldron, J.: A Rights-Based Critique of Constitutional Rights. Oxford Journal of Legal Studies 13(1), 18-51 (1993)
76. Nickel, J.: Making Sense of Human Rights. Blackwell, Malden (2007)
77. Eleftheriadis, P.: Legal Rights. Oxford University Press, Oxford (2008)
78. Edmundson, W.A.: An Introduction to Rights. Cambridge University Press, Cambridge (2012)
79. Hart, H.L.A.: Essays on Bentham: Studies in Jurisprudence and Political Theory. Clarendon Press, Oxford (1982)
80. Wenar, L.: Rights. The Stanford Encyclopedia of Philosophy (Fall 2015), http://plato.stanford.edu/archives/fall2015/entries/rights/
81. Waldron, J.: Dignity, Rights and Responsibilities. New York University School of Law. Public Law & Legal Theory Research Paper Series. Working Paper No. 10-83 (2010)