Not just user control in the General Data Protection Regulation. On controller responsibility and how to evaluate its suitability to achieve fundamental rights protection

Claudia Quelle

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

Keywords: data protection · user control · informational self-determination · controller responsibility · fundamental rights · autonomy · paternalism · will theories of rights · interest theories of rights

Abstract. User control is increasingly prominent in the discourse surrounding the General Data Protection Regulation (GDPR). However, next to 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 debate on the nature of rights. It concludes that a further exploration of will theories and interest theories of rights might shed light on the respective roles of user control and controller responsibility.

1 Introduction

Scholars differ of opinion as to whether the General Data Protection Regulation (GDPR) is and should be built on the right to informational-self-determination. Van der Sloot emphasizes that the focus on the individual and his rights to control is a recent development. He has found that 'the data protection rules originally could best be regarded as principles of good governance. The documents contained very broad and general principles of transparency and fair data processing, which were seen as the obligation and responsibility of the data processor. They were not framed as rights of the individual and not even linked to the private interests of data subjects, but rather to the quality and fairness of the process as such.'[1] On the other hand, Purtova would consider it radical to reject informational self-determination as 'a foundation of the European approach to data processing'.[2] While van der Sloot laments that the

adfa, p. 1, 2011.

GDPR is primarily founded on the philosophy of informational self-determination,[1] Purtova perceives a weakening of this principle because, amongst other reasons, the definition of consent has been tightened, despite the 'rhetoric of individual control' adopted by European politicians.[3] It will be argued below that the General Data Protection Regulation does emphasize and also strengthen the rights to control of data subjects, but that it also seeks to reinforce the fairness and due care exercised by the controller. Throughout the paper, controller responsibility is contrasted with user control.1 In my reading of the GDPR, controller responsibility sees to the notion that it is up to the primary norm-addressees of the General Data Protection Regulation – the controller – to ensure, through fair data processing practices, that the objective of data protection law to protect the fundamental rights of natural persons in the context of personal data processing is met. The tenet of user control seeks to give data subjects a measure of influence over the way in which their fundamental rights are protected.

The user control component of data protection has been emphasized during the data protection reform, but it has also 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 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][6] For a number of reasons, Matzner et al argue that the state should be responsible for granting citizens data protection.[5] Indeed, the normative argument can be made that data subjects should not be placed under the burden of regulating data processing operations and preventing unwanted consequences thereof, as this task befalls to controllers and their supervisory authorities. However, the question can be posed whether data protection is a responsibility of the state. Is the protection of fundamental rights of natural persons something which controllers, under the supervision of supervisory authorities, should take on for the benefit of the rights beneficiaries? And how should this question be researched?

First, the legal existence of the two tenets of user control and controller responsibility will be examined. Section two discusses the presence of user control and of controller responsibility in the General Data Protection Regulation. Section three enquires 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. Section four explores the virtues and drawbacks of a user control approach in light of the objective to protect fundamental rights, tying it to interest-based and will-based theories of rights. A dilemma is found: fundamental rights protection by others than the rights beneficiaries is (at best) based on the perceived interests of the beneficiaries (in this case, the data subjects), while to require them to express their interest might place a burden on them which they will not all be able to bear. This dilemma is tied to the debate on user control,

[1] Similarly, Borgesius distinguishes between rules that aim for control and rules that aim for protection.[4]

and particularly to Solove's charge of paternalism. Finally, in the conclusion, 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, proposed in January 2012 and to replace the Data Protection Directive from 25 May 2018, is increasingly presented as an instrument which seeks to strengthen user control in the travaux préparatoires. The Commission's Communication of 2010 started out paying fair heed to both user control and controller responsibility. It draws out this framework by emphasizing, first, that '[t]wo important preconditions for ensuring that individuals enjoy a high level of data protection are the limitation of the data controllers' processing in relation to its purposes (principle of data minimisation) and the retention by data subjects of an effective control over their own data.' It continued that data subject rights should be 'made more explicit, clarified and possibly strengthened', but also dedicated a section to its intention to 'explore ways of ensuring that data controllers put in place effective policies and mechanisms to ensure compliance with data protection rules'.[7] Two years later, 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'.[8] The Commission wants to 'put individuals in control of their own data'.[9] Anno 2016, recital 7 of the final GDPR states unequivocally that '[n]atural persons should have control of their own personal data'. On the date of its official adoption, rapporteur Jan Philipp Albrecht emphasises that '[c]itizens will be able to decide for themselves which personal information they want to share'.[10] However, behind the scenes his suggestion to add 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 Parliament.[1]

2.1 Consent and data subject rights

It is surprising that the role of user control ended up playing such a central role in how the General Data Protection Regulation was presented. A first tenet of data protection is indeed user control, 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 information – and in many cases, it is the only available legal ground (GDPR, art 9; ePrivacy Directive, arts 6, 9 and 13). Individuals are further granted a number of rights, including the right to be informed of a number of categories of information (GDPR, arts 12-14), to access, rectify or erase 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 of the

latter (arts 13(2)(b) and 14(2)(c)). The data subject rights do not only serve to grant data subjects 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 it is no longer necessary or if it has become unlawful to keep the data (art 17(1)). Further, as discussed in the next section, the right to be informed and to gain access to the data also shed a certain "sunlight" on the conduct of controllers. Importantly, the burden of proof regarding the right to object now unequivocally lies with the controller: 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 demanded by the level of specificity of a EU regulation, which does not require implementation by 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 latter additions serve to provide what Lynskey calls 'an architecture which bolsters individual control', to be distinguished from the control rights themselves.[11][2] This 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.

The General Data Protection Regulation tightens the definition of consent and strengthens its role. Consent must always be unambiguous, given either through a statement or a clearly affirmative action (art 4(11), recital 32).[3] Opt-out consent is never sufficient. When 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 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 demanded by the principle of transparency (art 12).[12] The condition that consent must be freely given was already present in the Data Protection Directive, but the GDPR adds that '[w]hen assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract' (art 7(4)). Recital 43 adds 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; and the provision of a good or service must not be made conditional on consent if the consent is not necessary for the performance of the contract. The data subject must be informed 'whether the data subject is obliged to provide the personal data and of the possible conse-

[2] However, Lynskey's architecture of "control" also sees to protective default settings and responsible data stewardship. [11]

[3] The Data Protection Directive also required consent to be unambiguous, but it was not yet part of the definition of consent, as a result of which consent required under the ePrivacy Directive needn't be per definition unambiguous.

quences of failure to provide such data' (art 13(2)(e)). Moreover, the special categories of data, for which explicit consent is required, are expanded (art 8). 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). As a result of these changes, consent will play a smaller, but more meaningful role in the data protection regime.

2.2 The data protection principles and controller responsibility

The second tenet of the GDPR, controller responsibility, was also strengthened through the addition of a large number of novel provisions. The data protection principles of Article 54 traditionally saw to good governance or due care; requiring that the processing of data is fair and reasonable.[1] Indeed, data protection law can be seen as a substantiation of the overarching principle to process data fairly and lawfully,[13, 14] which itself is a reflection of the requirements of good governance or fair administration in the public sector or due care in the private sector in the Dutch tradition [15]. According to Bygrave, 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. In addition, it also requires that controllers are transparent and do not unduly pressure data subjects into consent.[14]

It is the concern for the consequences of the processing which most clearly signals that the data protection principles are not only intended to make informational self-determination possible, although most of them undoubtedly also serve this latter purpose. In its famous decision establishing the right to informational self-determination, the Bundesverfassungsgericht already referred to purpose limitation as a means to ensure that there are clearly defined processing conditions which can be consented to [16], [26], cf [19]. Data minimization, storage limitation and integrity and confidentiality all require the controller to ensure that these conditions are kept to; that data is not kept longer than necessary or used in ways which were not necessary and that it is not accidentally processed in unauthorized or unlawful ways. These restrictions should ensure that the processing and its results align to the reasonable expectations of the data subject.[14] This is not only beneficial for informational self-determination; it also serves (or is supposed to serve [17]) as a limit on the processing, preventing the risks posed by aimless collection, unlimited dissemination, and misuse or arbitrary use of personal data.[18] The principle of storage limitation can help accommodate the insight that 'the quality of consent attenuates over time',[19] but it is first and foremost tied to the principle of purpose limitation (if the data is no longer necessary to serve the purpose, it must be anonymized or deleted). The transparency and information requirements towards the data subject make possible informed consent and the exercise of her rights,[12] but also serve to inspire fair

[4] The principles include lawfulness, fairness and transparency; purpose limitation, data minimization and storage limitation; and accuracy, integrity and confidentiality.

and reasonable processing operations: 'sunlight is the best of disinfectants' [20, 21]. It is noteworthy with regard to both tenets of the GDPR that the transparency requirements are made more specific, mentioning i.a. the legitimate interest, the storage period, the presence, logic and the significance and envisaged consequences automated decision-making, 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 for the processing to be fair, the GDPR specifies extensive requirements relating to both form and substance (arts 12-14), which are still to be supplemented under the principles of fairness and transparency, if necessary. Controller responsibility has been, and still is, present in the principles of data protection.

A great share of the novelties of the General Data Protection Regulation serve to strengthen the data protection principles, and in particular the second tenet of controller responsibility. Many of them are to be found in Chapter IV, which asks controllers to take technical and organisational measures to implement the data protection principles and to protect the rights of data subjects, whereby they have to limit the processing to what is necessary in accordance with the data protection principles by default (art 25);5 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); and to assess and find ways to mitigate high risks to the rights and freedoms of individuals posed by their processing activities (art 35). Note that these obligations require controllers to engage in fair practices and prevent harm without any involvement on the part of data subjects. Rather; protection has to be provided upfront and by default – data subjects should not need to ask for it. Controller responsibility does, of course, take place under the supervision of regulatory agencies. Chapter IV further asks controllers to be able to demonstrate compliance (art 24), to employ and involve a data protection officer (arts 37-39), and to translate data protection law to practice through codes of conduct which can be certified (arts 40-43). Although the general duty to notify supervisory authorities has been abolished, it has been replaced by processes which will hopefully shift the attention of the authorities to more risky cases and enable them to gauge the situation at hand more readily (arts 6(1)(a), 7, and 9(2)(a)). Article 83 introduces fines up to 20 000 000 EUR or 4 % of the total worldwide annual turnover of an undertaking. Nonetheless, the system as a whole is meta-regulatory; it regulates how controllers regulate themselves, and as such is an appropriate accompaniment to a data protection system which is driven by the open norms of fairness and due care - requiring controllers to determine not only whether to rely on consent or on another legal ground (arts 6 and 9) or to store data in case the data subject wishes to retrieve it through an access request (art 15)[23] (examples pertaining to user control), but also whether their purpose or interest outweighs the possible consequences for the interests and fundamental rights of data subjects (arts 6(1)(f) and 6(4)(d)), how to mitigate risks to the rights and freedoms of individuals posed by their

[5] Data protection by design and by default is also related to control in an important way. Lazaro and Le Métayer note that 'control becomes almost impossible when the data subject has to deal with privacy-unfriendly default settings and technologies'. [22]

data processing operation (art 35(7)(d)), and at what point their security measures are appropriate given the level of risk (art 32(1)) (examples of controller responsibility). 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. 'Responsibility for such compliance had always fallen on their shoulders, irrespective of whether somebody was looking, or whether somebody complains'.[24] 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'[14] what that entails if she wants to.

3 Proposal to evaluate user control and controller responsibility in light of fundamental rights

3.1 User control or controller responsibility – to what end?

Evaluations of user control are fraught with conceptual difficulty. As perceptively remarked by Lazaro and Le Métayer, it is important to distinguish between user control as part of the foundation of data protection ('the conceptual dimension of control') and user control as private enforcement ('its instrumental dimension')'.[22] Purtova highlights that, as data processing became increasingly prevalent, private enforcement options (i.e. right to object and rights of complaint) were introduced to overcome the failing of a purely administrative set of rules.[2] While there is a clear link, this instrumental dimension must be separated from the matter of the ends which such enforcement serves. Whether private enforcement is a welcome addition, brought about as a by-product of the data subject's rights to be granted access to justice and to seek redress, or whether it is essential to the goal of data protection, depends on how the foundation and objective of data protection is conceptualized (and, as will be argued in section 4, on how rights are conceptualized). Data protection law consists of different facets, foundations, or goals, which scholars disagree on and which do not all support the same conclusion on the appropriate division of responsibility. In my opinion, it follows from the analysis in section 2 that the General Data Protection Regulation places heavy reliance on enforcement by both private and supervisory authorities (instruments) 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 different kinds of unjustifiable harm (goals). I will first discuss the protection of interests of the data subject, paying particular attention to her ability to construct her identity in 'a zone of relative insulation from outside scrutiny and interference'[19], as this will feature in the discussion on constraints on freely and autonomously provided consent in section 4.1. Next, I will discuss informational self-determination, which protects the ability of data subjects to decide on the dissemination of information relating to her and is frequently seen as the justification for the tenet of user control.

When Matzner et al argued that it is not normatively desirable 'to choose the individual user as the main responsible actor to improve the state of data protection',[5] their focus was on a secrecy-oriented conception of the protection of personal data. This clearly identifies an interest which can 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 (see e.g. recital 75, which identifies a number of risks or sources of risk). More generally, the GDPR seeks to ensure that the controller takes the interests of data subjects into account and to prohibit unjustifiable risk-taking. Under such a conceptualization of the objectives of data protection, it is not necessarily essential that data subjects have control rights. In my view, the concern about identity construction also identifies a need or interest which can be protected by controllers. A number of theories of privacy focus on the self-construction of data subjects, for example in relation to profiling. The regulation of profiling is often tied to the loss of control of the data subject, as new data is inferred which the data subject did not choose to disclose.[26] It can also harm the data subject in ways counter to her fundamental rights, as when a candidate is not hired because her future work performance is predicted on the basis of ethnicity (cf GDPR, recital 71). Some scholars are particularly concerned about the impact of the use of profiles for personalisation on one's ability to construct one's identity. For example, Cohen takes particular issue with her observation that 'networked individuals move within personalized "filter bubbles" (Pariser 2011) that both nudge them in profit-maximizing directions and conform the information environment to their political and ideological commitments. Modulation shapes and produces preferences for choices to be presented—choices not only among goods and services, but also among information sources, facts, theories, and opinions. Meanwhile, interdiction takes other options off the table, foreclosing prohibited or undesirable interactions with cultural artifacts and forms. This twofold process aims to produce a particular kind of subject, the citizen-consumer, "whose preferred modes of self-determination play out along predictable and profit-generating trajectories"'.[29] There are multiple theories of privacy which, like Cohen's, view privacy as granting individuals a private zone within which they can consciously and with relative autonomy engage in self-formation.[30, 31, 32] Such concerns relating to the self-formation versus the shaping of individuals are logically accompanied by a different division of responsibility. Certain interferences with our process of self-formation simply should not be undertaken; this is primarily a duty of controllers.

User control and controller responsibility play a different role in data protection if the focus is on the right to informational self-determination, as conceived in the German tradition. Control is also central to Westin's well-known conceptualisation of privacy. It was of great influence to the EU data protection tradition that the Bundesverfassungsgericht brought to life the right to informational self-determination in a 1983 ruling, translated by Rouvroy and Poullet 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'. Underlying this right is a concern about chilling effects – for example, if a citizen is forced to register officially for participation in an assembly she might renounce

the exercise of this right –,[25, 26, 27] but the court must have considered it so essential that an individual have control over information flows to achieve this aim that the control as such was granted protection by a right of its own. When looking at this right in isolation, the responsibility of controllers and state regulators would be limited to what is necessary to enable data subjects to determine the limits of data flows regarding themselves. Thus, with regard to the enforcement of data protection, Purtova notes that data protection regulation was adapted to restore 'the balance of power between individuals and data processing actors'.[2] If control rights are unenforceable because of the complexity of the Big Data landscape,[28] the right to informational self-determination would theoretically demand state intervention to remedy the situation. Next to the pre-conditions for effective control by data subjects, however, controllers would only be under further obligations if the right to self-determination is subject to an interference, so as to make the interference proportionate.6

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

How to engage in an evaluation of the roles of user control and controller responsibility in data protection, if its two main facets point in different directions? Are we forced to rely on farfetched interpretations of context-specific CJEU cases and EDPD opinions to highlight one facet or the other, ignoring the complex whole of the GDPR? This paper proposes to ask the question of responsibility with regard to fundamental rights in general. While this does not pay due attention the particular role played by informational self-determination (countering chilling effects), it does reflect the legal state of affairs and, as will become clear in section 4, it also ties in well with the debate on user control.

Overarching the different tenets of the GDPR, is the objective to protect fundamental rights. According to 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. Recital 4 reminds us that '[t]he right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular 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,

[6] The Bundesverfassungsgericht allows limitations on the control of individuals if the public interest weighs heavier. The existence of exceptions must be provided by law and proportionate; a leading factor is the possible use of the data, whereby the court also had an eye on the possible harms of the use. With regard to data collected for statistical purposes, it mentioned the possible risk of social stigma involved in processing data relating to, for example, addiction, mental health, and criminal records, as an important consideration (par 167). [16]

the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.' In other words, when the EU legislature decided to substantiate the meaning of the right to the protection of personal data through secondary legislation, it was fully aware that not one right could take priority in the resulting legal framework.[e.g. 33] This can also be seen in the frequent reference made to "the rights and freedoms of individuals" throughout the GDPR, which must be understood as referring to not only privacy, but also 'other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion'.[34]

This recognition of other rights and freedoms ties in well with Nissenbaum's theory that some data flows are appropriate and others are not – a decision which is not wholly dependent on the amount of secrecy or control which is provided.[35] Some scholars even 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'.[36, 37, 38] In other words, data protection law provides channels for the coordination of different rights, through which controllers should 'reconcile fundamental but conflicting values such as privacy, free flow of information, the need for government surveillance, applying taxes, etc'.[39]7 This focus on balancing not only accommodates the fact that privacy is not of higher rank than other fundamental rights; it is also able to bring in the leeway required in the European Union to allow Member States to protect rights in accordance with their constitutional traditions.

One of these other values is the free flow of data. At the same time as setting out the protection of fundamental rights as the main objective, Article 1 GDPR also 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 EU focus on the establishment of an internal market. At this point in time, the EU should 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 that increasingly commits itself to the political project of protecting fundamental rights'.[42] Thus, 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 (GDPR, recital 9).[9] Nonetheless, the CJEU pays less and less attention to the internal market dimension.[11][40] Lynskey 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.[11] I agree that the focus should on the overarching objective to protect fundamental rights, although we should recognise that the free flow of information can be one of the competing interests which needs to be taken on board when the balance between the relevant rights and interests is struck.

---

[7] Note, however, that Gellert, De Hert and Gutwirth have developed their view on EU data protection from a Belgian background, and that, according to González Fuster, Belgium is one of the Member States 'where the protection of personal data is conceived as primarily serving other existing rights'. [27]

It could be argued that the notion of "fundamental rights" is very thin in the EU, and is therefore incapable of offering a suitable normative framework. In the EU, the question of what fundamental rights entail and why they should be granted by the EU has revolved around the boundaries between national constitutional traditions and the newfound EU fundamental rights framework.[e.g. 41] The authority of the EU to decide what its fundamental rights entails is actively contested by several Member States. In the words of Augenstein, 'it is the absence of a European equivalent to a national constitutional tradition that engenders the very debate about the autonomous interpretation of EU fundamental rights law', as a result of which 'conflicts of authority between the EU and the Member States ('who decides?') perpetuate themselves in difficulties to determine the autonomous substance of EU fundamental rights law under conditions of political disagreement ('what counts as a good decision?')'.[42] It is telling that fundamental rights adjudication itself has been cast in terms of a dialogue between the EU Court of Justice and the courts of Member States.[e.g. 43] This state of affairs only opens the door to non-legal interpretations of what fundamental rights entail, and is not at all at odds with the conclusion of the article that further research should look to philosophical debates on whether rights should be interest-based or choice-based.

4 The "choice" to consent and the "paternalism" of protective legislation in light of fundamental rights

Not only does the proposal to see the responsibility question as an issue of fundamental rights do justice to the legal context of the GDPR, it also ties in well with the current debate on the problems with and virtues of a notice-and-consent system. In the following, the debate about user control is presented as pertaining to the significance of constraints on the free and autonomous choice of data subjects and the permissibility of state intervention for the perceived benefit of the data subject. Next, a parallel is drawn with a core dilemma in fundamental rights and human rights theory.

4.1 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 these concerns are about constraints on the ability of individuals to freely and autonomously make an informed choice about the data processing opinion. Choice always occurs under a set of conditions or parameters. In the words of Cohen: '[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'.[19] Benn clarifies that the conditions also relate to states of the agent, distinguishing between the resources which are available, the opportunity costs involved in pursuing X, the goals of the agent in light of which the choice is made, and the beliefs the agent holds about there conditions. Restrictions of freedom can result from restrictions with regard to all four conditions.[44] Many data protection

scholars think the restrictions are such that we can no longer speak of a real choice. Now the issue is that, despite these constraints, consent is still considered informed and freely given – and it remains to be seen to what extent the changes to the consent regime in the GDPR will make a difference in ameliorating the constraints and/or considering consent invalid because of their existence. In the following, I will group the constraints in three related categories, mostly for the sake of overview and presentation rather than for conceptual clarity.

Firstly, data subjects do not have enough time to consider each processing operation, because they engage with services which collect data so frequently. Or, put slightly differently, they at least lack the will to make time for this burden – and understandably so, considering how uneconomical it would be.[45, 46] While this problem can be attenuated by grouping together different types of processing operations, this also lumps together different situations, in which different values and interests may play a role. 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. Big data analytics may not even be explainable in human language. Data can also be inferred from other available data, so that data shared by others can be used to infer things about you.[45], [47-48] This makes it very difficult to adequately estimate the effect of the choice to share this one piece of information. The information (including information on the logic employed by self-learning algorithms and the other data sources which will be accessed) could be presented in accessible and less time-consuming ways, for example through logo's or seals, but this 'conflicts with fully informing people about the consequences of giving up data, which are quite complex if explained in sufficient detail to be meaningful'.[45] Or, in the words of Koops, '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.[28] The first two types of concern exist quite apart from the actual practices of notice and consent, which only make matters worse. Notices are long and couched in inaccessible language,[49] yet fail to shed light on the often complex 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.[50]

The third problem relates to more or less imposed constraints to the freedom and autonomy of choice. Data subjects may be faced with nonnegotiable or excessive "terms", under which they are asked to surrender a great deal of personal information, while they are unable to get the desired goods or services elsewhere under more reasonable terms. 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'.[28] Further, there may well be all kinds of pressures which lead the data subject to desire the product or service. Matzner et al remind us of the costs involved in not owning a smart phone: 'less contacts with friends, missing carrier 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'.[5] Rouvroy and Poullet worry about socio-economic and other structural inequalities which are difficult to address through data protection legislation.[25] The situation is grave enough for Hull 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.[51] Cohen also does not mince words, pointing to the power exercised through 'public and private by private regimes of surveillance and modulation' to turn us into 'citizen-consumers'.[32] Together with other scholars, she mentions our biases and bounded rationality, apparently perceiving them as cracks through which government and corporate actors manipulate our choices.[29], [45, 46], [51] She 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'.[19]

4.2 The "paternalism" of protective legislation

The problems described above all present 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 OK operations which might cause them harm. But does this mean that their interests should be formulated and defended for them? Solove is not ready to make this jump. On the one hand, Solove recognises these constraints and concludes that '[c]onsent to collection, use, and disclosure of personal data is often not meaningful'. On the other hand, he also 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.[45] Indeed, proponents of privacy self-management argue that, through a system of user control, 'everyone may attain his own desired level of data protection'.[1] While this is too simple a picture, as there are interdependencies and inequalities — e.g. the data one person shared can be used to profile another, and some groups may be more pressured to share their data than others — [5],[8] 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 protectionist or paternalist because of the many rules which restrict processing even in the

[8] Matzner at all 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, e.g. that it is more important for young women in the achievement of social success to share private things, such as bikini shots, on Facebook.[5]

absence of any wish or claim on the side of the data subject.[45] And while it could definitely be argued that many of the EU rules are necessary preconditions to meaningful consent (see sections 2.2 and 3.1), the GDPR also entails a weighing of the interests and rights at stake by the controller and its supervisory authority for the (perceived) benefit of the data subjects and society as a whole.

The charge of paternalism points to the heart of the debate. Paternalism can be understood as 'the usurpation of one person's choice of their own good by another person'.[52] Paternalism is not necessarily a bad thing. As indicated in the following section, it might actually be what the protection of one's rights requires under an interest-based approach. For now, however, it will be assumed that the rule one has over oneself is of such importance that paternalist actions cannot be accepted. Now, if the GDPR or specific rules or provisions of the GDPR were enacted for the main reason to protect third parties and society as a whole against the harmful choices which individual data subjects would make in a market-based system of privacy self-management, the charge of paternalism would not apply.[53] It is worth researching to what extent this is the case. On the one hand, a concern for the interests of the data subject and the risks or possible consequences for the data subject is present in the principle of fair processing and throughout the rest of the GDPR. It is safe to assume that this side of data protection is as paternalist as the prohibition on the manufacture of cigarettes for the protection of the individual consumers who would pick up smoking.[54] On the other hand, the legal grounds next to consent and contract all, directly or indirectly, pertain to the interests of others or the public interest. Third party interests should have a place in data protection law, as the data of one person can be used to infer information about other people [5], and can also be used for the benefit of others. It has also 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 individual data subjects.[1]

A further issue in applying the "paternalism" label pertains to the role of choice. According to Archard, it is necessary that the paternalist P discounts Q's belief that P's behaviour does not promote Q's good.[52] The same applies if she would have disagreed with the intervention if she had known.[53] Thus, it seems that people who oppose or would the data collection practices they do end up consenting to, could be protected without the charge of paternalism. However, according to Shiffrin's conception, even if the data subject did not believe the exchange to be in her benefit, but was weak-willed and agreed anyways (e.g. for the sake of convenience), the intervention would classify as paternalist.[55] Protecting people from the "privacy paradox" would then also count as paternalism. On the other hand, if the state thought that the data subject would want it to intervene, while she would in fact not authorize the intervention, Archard would qualify it as misguided beneficence instead.[52] The situation is even less clear-cut if the data subject has not formed a conscious, autonomous choice. In that case, her autonomy is not impinged, but her freedom would nonetheless be restricted by the intervention. Note that while a choice can be formed more or less reflectively or deliberately, meaning that autonomy is gradual, a person is often morally and legally granted the liberty of 'a valid decision-making body' if she meets a certain threshold of rationality, self-reflection and self-control.[56], [44] While it is

now popular in data protection scholarship to 'question the very possibility of control by deconstructing the conventional figure of the "rational and autonomous agent" that is at the core of "privacy as control" theories',[22] only a certain "amount" of rationality and autonomyis needed to sustain the tenet of user control - and even Foucault believed that "as soon as there is a power relation, there is the possibility of resistance'.[57] The question is whether the average data subject who could not take the time to find and read an incomprehensible privacy policy and 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.9 And if the answer is no, the follow-up question is whether this means that her freedom can be restricted, or whether her "choice" should be respected nonetheless.

4.3 Allocating responsibility for fundamental rights protection

Considering that the main, overarching objective of the GDPR is the protection of the fundamental rights of natural persons, the question about responsibility is as follows: Is the protection of fundamental rights of natural persons something which controllers, under the supervision of supervisory authorities, should take on for the benefit of the rights beneficiaries? First a word on fundamental rights. Fundamental rights are determined by, apply in, and give direction to a given polity. In the words of Palombella, 'fundamental rights are to be understood as encompassing those selective and substantive criteria which, together with others, enable judgments of "validity": the recognition of belonging to a legal order, legitimacy, compatibility of institutional behaviour and norms within a given legal—political system'. The fundamental rights of a polity protect those goods which are deemed fundamental in or by that polity, and 'if they are goods deemed to be fundamental, then they are protected, fostered and pursued with the available means as principal objectives not only of the courts but also of all institutions'.[58] At first sight, at least from a legal perspective, 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 fundamental rights. The constitution of a state can legally require it to act or to refrain from taking action, including through the regulation of corporate conduct. However, one can wonder whether the protection of fundamental rights is a task which the state (and by proxy, corporations) should fulfil. The matter of rights becomes more complicated if one recognizes, with Waldron, that '[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

[9] Similarly, consumer law sees consumers as reasonably well-informed, observant and circumspect, which strikes a particular 'balance between the need to protect consumers and promoting free trade'. González Fuster thinks that in data protection law, the data subject is not regarded as well-informed, although I am not sure I agree; the problem which the EU institutions are grappling with, is rather that the law readily assumes that they are informed, while in reality they are not. [12]

considerations'.[59] [42] This gives the concern over paternalism a particular sting, as it affects not only the freedom and autonomy of an individual, but also his or her say regarding the substance of fundamental rights protection in her polity.

The answer on the question of responsibility will differ depending on whether a will-based theory or an interest-based theory of rights is adopted. Simplifying a complex debate, the following indications will suffice to show that this is a relevant area for further research. Interest or benefit theories see it as the function of rights to promote interests by giving the rights-holder the benefit from another's duty. The idea is that some interests merit special attention. A right exist because there is an interest which requires protection. These interests could be shared interests which every human needs or wants to see met. The standard could be, for example, that of the minimally good life.[60] 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'.[61] If, however, 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, we could speak of paternalism. The problem, as hinted at in the quote of Waldron above, is that there may be a discrepancy between the interests one is perceived to have and the interests one has or wishes to see defended. This is also what Solove takes issue with regarding the protection offered by EU data protection law in the absence of a claim made by a data subject. Note that for this situation to occur, it is necessary that rights are respected "by default", i.e. without having been claimed. In many cases, the duty one owes as the correlate of someone else's right should be respected without a claim having been made. In other words, I must act responsibly, in a manner which respects the rights of others. As observed by Bix, 'When I drive my car, post a comment on Facebook, or run a business, I need to do so responsibly, in the sense that my actions must respect the liberty, property, and reputational rights of others, or risk civil, and perhaps even criminal, liability if I do not'.[62] The fact that rights are respected "by default" also entails that individuals who lack the freedom, autonomy or agency to claim their rights, are protected. However, it also 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 interest.

Will or choice theories, on the other hand, see the function of rights not as the protection of one's interests (unless perhaps the interest is that of autonomy[63]), but in granting the right bearer control over another's duty.[64] '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.'[65] The purpose and value of rights lies in this exercise of choice. As a consequence, the rights holder can waive, annul or transfer these duties; the right is at their disposition. Paternalism is not a problem, as the rights holder can claim or waive a right in case he or she disagrees with the behaviour of the duty-bearer. However, will theory leaves incompetent or non-autonomous human beings without protection since they do not have the ability to dispose of their rights; they would not even qualify as a rights-holder. This forces the will theorist to resort to proxies which can exercise power for them, such as parents or legal guardians.[63] 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 [63]), or only to those who have made a conscious, autonomous choice – and where to draw the line. Another issue in the debate on user control is also able to make an appearance. If data protection law is about protecting society as a whole or arranging data flows in light of interdependencies and inequalities rather than about giving individuals control, then under a will-based account, rights are not necessarily a suitable means to achieve this aim; there would be no use in according individuals a sphere in which they should have control, unless this is regarded as their individual expressions of the appropriate direction of fundamental rights protection with regard to the processing of personal data for the polity as a whole.

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 General Data Protection Regulation 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. It brought to the fore a dilemma which is present in the debate on "notice-and-consent" and which ties in well to the debate between will-based and interest-based rights theories. Ideally, the data subject is able to decide on the appropriateness of the data processing activity in light of the balance between the applicable rights and interests which they think should be struck. However, the constraints on her ability to do so freely and autonomously might lead her to inadequately defend their fundamental rights, as it limits her capacity to understand what a data processing operation might entail for, say, their right not to be discriminated. Thus, there is something to be said, on the one hand, for placing the responsibility for the protection of fundamental rights primarily with the beneficiaries of rights protection: the data subjects. This enlarges the legal power available to data subjects to partake in the formulation of the meaning of fundamental rights in specific situations. Moreover, to protect them against their will readily constitutes paternalism. On the other hand, it would place too large a burden on individual data subjects to expect them to make a well-considered, autonomous choice, in which they come to the choice which matches their interests, needs and preferences in resistance to external pressures to become a "citizen-consumer", so that the more protective tact of controller responsibility gains attractiveness. To simplify a complex dilemma: the controller and its supervisory authority can intervene with (hopefully) what they perceive to be the interests of data subjects and society as a whole at heart, or the state can try to enable data subjects to defend their interests themselves, although they will not always be able to do so. This very dilemma can be further analysed, and possibly answered, in light of will- and interest-based theories of rights on the fronts of paternalism and the rights of the incompetent or non-autonomous. To over-simplify: if the rights of the data subject serve to protect her interest, the bullet of paternalism is easily bit; on the other hand, if their rights require them to engage in an active expression of their preferences or choices, any

further protection cannot occur in the name of (fundamental) rights. In the meantime, we must surely prevent two things. First, that dishonest appeals made by controllers to either informational self—determination of data subjects or to the benefits of their activities, made only so as to expand their activities and increase efficiency and economic growth, are taken at face value. Second, that a lack of engagement by data subjects is used to legitimize data processing operations which are detrimental to society.

References

1. 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)
2. Purtova, N.N.: Property rights in personal data: A European perspective. BOXPress BV, Oisterwijk (2011)
3. 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)
4. Zuiderveen Borgesius, F.J.: Improving privacy protection in the area of behavioural targeting. PhD thesis, University of Amsterdam, Amsterdam (2014)
5. 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)
6. O'Mailey,P.: Responsibilization. In: Wakefield, A., Fleming, J. (eds): The SAGE Dictionary of Policing. SAGE, London (2009)
7. European Commission: Communication on personal data protection in the European Union. COM(2010) 609 final
8. European Commission: Impact Assessment accompanying the General Data Protection Regulation. SEC(2012) 72 final
9. 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
10. European Parliament, http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era
11. Lynskey, O.: The Foundations of EU Data Protection Law. Oxford University Press, Oxford (2015)
12. 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)
13. Bainbridge, D.: Introduction to Computer Law. Pearson Longman, Harlow (2004)
14. Bygrave, L.A.: Data Privacy Law. Oxford University Press, Oxford (2014)
15. *Kamerstukken II* 1997/98, 25892, 3

16. BVerfGE 65, 1 – *Volkszählung*
17. 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 Digitalis. Preadviezen 2016 Nederlandse Juristen-Vereniging, pp 9-124. Kluwer Juridisch, Deventer (2016)
18. 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)
19. 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)
20. 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)
21. 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)
22. Lazaro, C., Le Métayer, D.: Control over personal data: true remedy or fairytale? SCRIPT-ed 12(1), 3-34 (2015)
23. Case C-553/07 Rijkeboer [2009] ECR I-293
24. 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
25. 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)
26. 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)
27. González Fuster, G.: The emergence of personal data protection as a fundamental right of the EU. Springer, Cham (2014)
28. Koops, B.J.: The trouble with European data protection law. International Data Privacy Law (2014)
29. 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
30. Richards, N.M.: Intellectual Privacy. Texas Law Review 87, 387-445 (2008)
31. Schwartz, P.M.: Internet Privacy and the State. Connecticut Law Review 32, 815-857 (2000)
32. Cohen, J.E.: What Privacy is For. Harvard Law Review 126, 1904-1933 (2013)
33. Joined cases C-92/09 and C-93/09 Volker und Markus Schecke [2010] ECR I-11063
34. Article 29 Data Protection Working Party: Statement on the role of a risk-based approach in data protection legal frameworks. WP218 (2014)

35. Nissenbaum, H.: Privacy as contextual integrity. Washington Law Review 79, 119-158 (2004)
36. 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)
37. 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)
38. Gellert, R., Gutwirth, S.: The legal construction of privacy and data protection. Computer Law & Security Review 29, 522-530 (2013)
39. 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)
40. 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)
41. Sarmiento, D.: Who's afraid of the Charter? The Court of Justice, national courts and the new framework of fundamental rights protection in Europe. Common Market Law Review 50(5), 1267-1304 (2013)
42. Augenstein, D.H.: Disagreement – Commonality – Autonomy: EU Fundamental Rights in the Internal Market. Cambridge Yearbook of European Legal Studies. 15, 1-26 (2013)
43. Perez, A.T.: Conflicts of Rights in the European Union: A Theory of Supranational Adjudication. Oxford University Press, Oxford (2009)
44. Benn, S.I.: Freedom, Autonomy and the Concept of a Person. Proceedings of the Aristotelian Society, New Series, vol. 76, 109-130 (1975-1976)
45. Solove, D.: Introduction Privacy self-management and the consent dilemma. Harvard Law Review 126, 1880-1903 (2013)
46. 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)
47. 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)
48. 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)
49. Article 29 Data Protection Working Party: Opinion 10/2004 on More Harmonised Information Provisions. WP 100 (2004)
50. 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)

51. 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)
52. Archard, D.: Paternalism Defined. Analysis 50(1) 36-42 (1990)
53. Bullock, E.: A normatively neutral definition of paternalism. The Philosophical Quarterly 65, 1-21 (2015)
54. Dworkin, G.: Paternalism. The Stanford Encyclopedia of Philosophy (Summer 2016), <http://plato.stanford.edu/archives/sum2016/entries/paternalism/>.
55. Shiffrin, S.V.: Paternalism, Unconscionability Doctrine, and Accomodation. Philosophy & Public Affairs 29(3) 205-250 (2000)
56. Fateh-Moghadam, B., Gutmann, T.: Governing [through] Autonomy. The Moral and Legal Limits of "Soft Paternalism". Ethical Theory Moral Practice 17, 383-397 (2014)
57. Heller, K.J.: Power, Subjectification and Resistance in Foucault. SubStance 25(1), 78-110 (1996)
58. Palombella, G.: From human rights to fundamental rights: on the consequences of a conceptual distinction. EUI Working Paper LAW No. 2006/34, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=963754
59. Waldron, J.: A Rights-Based Critique of Constitutional Rights. Oxford Journal of Legal Studies 13(1), 18-51 (1993)
60. Nickel, J.: Making Sense of Human Rights. Blackwell, Malden (2007)
61. Eleftheriadis, P.: Legal Rights. Oxford University Press, Oxford (2008)
62. Bix, B.H.: Rights, Responsibilities, and Roles: A Comment on Waldron. Arizona State Law Review 43, 1137-1149 (2011)
63. Edmundson, W.A.: An Introduction to Rights. Cambridge University Press, Cambridge (2012)
64. Hart, H.L.A.: Essays on Bentham: Studies in Jurisprudence and Political Theory. Oxford: Clarendon Press (1982)
65. Wenar, L.: Rights. The Stanford Encyclopedia of Philosophy (Fall 2015), http://plato.stanford.edu/archives/fall2015/entries/rights/