Journal of Consumer Policy (2019) 42:91–107
https://doi.org/10.1007/s10603-018-9399-7

ORIGINAL PAPER

Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective

I. van Ooijen[1] · Helena U. Vrabec[2,3]

Received: 8 May 2018 / Accepted: 20 November 2018 / Published online: 11 December 2018

Abstract
Because of increased technological complexities and multiple data-exploiting business practices, it is hard for consumers to gain control over their own personal data. Therefore, individual control over personal data has become an important subject in European privacy law. Compared to its predecessor, the General Data Protection Regulation (GDPR) addresses the need for more individual control over personal data more explicitly. With the introduction of several new principles that seem to empower individuals in gaining more control over their data, its changes relative to its predecessors are substantial. It appears, however, that, to increase individual control, data protection law relies on certain assumptions about human decision making. In this work, we challenge these assumptions and describe the actual mechanisms of human decision making in a personal data context. Further, we analyse the extent to which new provisions in the GDPR effectively enhance individual control through a behavioural lens. To guide our analysis, we identify three stages of data processing in the data economy: (1) the information receiving stage, (2) the approval and primary use stage, and (3) the secondary use (reuse) stage. For each stage, we identify the pitfalls of human decision-making that typically emerge and form a threat to individual control. Further, we discuss how the GDPR addresses these threats by means of several legal provisions. Finally, keeping in mind the pitfalls in human decision-making, we assess how effective the new legal provisions are in enhancing individual control. We end by concluding that these legal instruments seem to have made a step towards more individual control, but some threats to individual control remain entrenched in the GDPR.

Keywords Individual control · EU data protection law · GDPR · Decision-making · Behavioural economics

✉ I. van Ooijen
i.vanooijen@utwente.nl

Extended author information available on the last page of the article

Individual Control and the GDPR

The progressing of the information age has led to an increase in online transactions concerning consumer data. Because of increased technological complexities and multiple data-exploiting business practices, it is becoming harder for consumers to gain control over their own personal data. Observing these trends, behavioural scientists have warned for a number of threats to individual control, such as information overload and data invisibility (Kamleitner and Mitchell 2018).

In legal theory and practice, the important role of individual control did not go unnoticed. It has been considered desirable that individuals are able to exert some form of control over their personal data. That is, individual control, in particular with regard to one's person, has been described as a reflection of fundamental values such as autonomy, privacy, and human dignity (Koops et al. 2016; Mantelero 2013; Nissenbaum 2004; Solove 2007; Westin 1968). The German constitutional court's judgement on the population census well illustrates the importance of control over data on the fundamental right level (Bundesverfassungsgericht 1983). The Court noted that "… If someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu and cannot estimate sufficiently the knowledge of parties to whom communication may be possibly be made, he is crucially inhibited in his freedom to plan or to decide freely and without being subject to any pressure influence." (p. 171)[1]. In the holding, the Court described this ability to exercise the freedom to decide as "control" and indicated that it could be easily compromised in the context of modern data processing. Indeed, the data-driven economy has generated an environment in which the data barons (i.e., big companies, government agencies, intermediaries) have a unique control over digital information, which is no longer counter-balanced by control of other actors (Mantelero 2014).

The General Data Protection Regulation (GDPR; Directive (EU) 2016/679) is a recently developed legal instruments in the European Union (EU) that regulates processing of personal data in the EU. In the GDPR, the need for individual control seems to be addressed more explicitly and with greater prudence compared to earlier regulations. In fact, strengthening individual control was one of the key goals of the EU legislator, as expressly laid down in the policy documents preceding the GDPR proposal (Reding 2011) and in the text of the GDPR itself.[2] In spite of the fact that the GDPR dedicates a great deal of attention to data subjects' control, they have been often criticized by behavioural scientists for not being able to address these threats appropriately. Take some simple examples: Data controllers are required to put a policy on their websites to inform consumers about privacy risks, but many consumers do not understand them. Further, data subjects should be given an option to express consent to data processing, but they often do not seem to think through the consequences of providing (or refusing) consent. Rather, they simply consent whenever confronted with a consent request (Custers et al. 2013). With the growth of invasive digital technologies and algorithmic decision-making, the challenges for control over data have become even greater (Cohen 2018).

On the mission to enhance individual control, we believe that it is important to take into account the psychology of information processing and decision-making. By evaluating the GDPR through a behavioural lens, it is possible to predict its effectiveness in terms of *actively enhancing* individual control. Considering the serious concerns in relation to the modern personal data processing, such an assessment is highly needed. Therefore, the contribution of this paper is to critically examine the

[1] The English translation of the judgement is available at: https://freiheitsfoo.de/files/2013/10/Census-Act.pdf.
[2] See for example recitals 7 and 68.

EU mission to enhance individual control in the data-driven economy by assessing the effectiveness of the GDPR from a behavioural perspective. We conceptualize individual control as *the extent to which an individual is consciously aware of a situation and has the conscious intention and the ability to start, stop or maintain a situation* (see also Bargh 1994).

To guide our assessment, we identify three stages of a typical consent-based data processing in the (big) data economy: (1) the information receiving stage, (2) the approval and primary use stage, and (3) the data secondary use (reuse) stage (see Fig. 1). In the *information receiving* stage, data collectors provide the individual with information by means of a user policy or a similar piece of information. In the *approval and primary use* stage, the context wherein decisions about personal data are made, as well as the manner in which data collection requests are framed, affect individual control. The third stage concerns *secondary uses of data*. Here, we discuss how certain affordances of digital data, such as intangibility and invisibility, further limit individual control. We pay special attention to the fact that the situation has been exacerbated in the growing data-driven economy.

We state that each stage is associated with certain pitfalls that result from cognitive processing and human decision-making, which pose threats to individual control over personal data. For each stage, we explain the pitfalls in cognitive processing and human decision-making, and subsequently explain how newly introduced principles in the GDPR address these issues. Thus, our aim is not to provide an exhaustive overview of the extent to which the GDPR's provisions, including similar provisions that exist within its predecessors, enhance individual control. Rather, we focus on the newly introduced principles in EU privacy law that aim to empower consumers in their control and assess to what extent they enhance individual control from a behavioural perspective (Table 1). We end with concluding on the effectiveness of the GDPR in enhancing actual individual control over personal data.

Provisions in the GDPR That Are Related to Control

The General Data Protection Regulation (GDPR), the EU core data protection statute, contains several references to individual control. For instance, in (the non-binding) Recital 7, it is

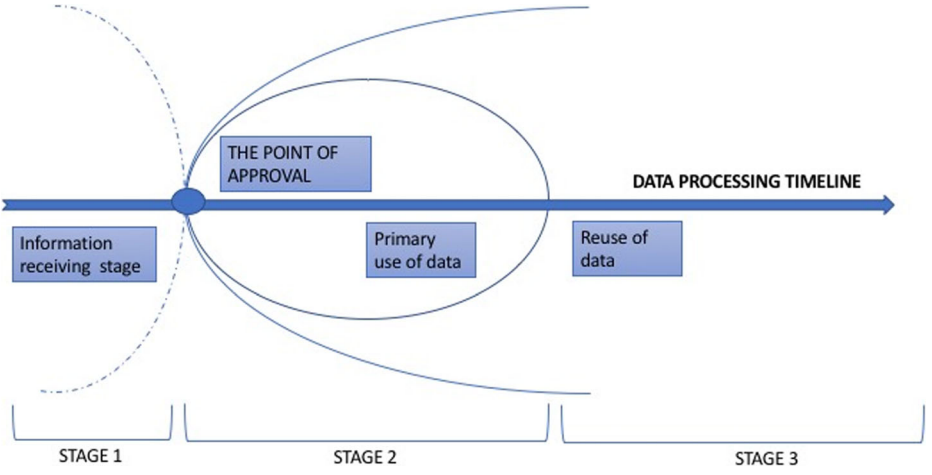

Fig. 1 Graphical representation of the typical consent-based data processing timeline

mentioned that "Natural persons should have control of their own personal data" (p. 2). Furthermore, the idea of control over personal data also comes to front in the provisions on consent and in the provisions on data subject rights.

Consent represents one of the six legal bases of data processing.[3] By consenting, an individual approves that her data is used for one or more specific purposes. Data subject rights, also referred to as subjective rights or control-rights (Lynskey 2015), are a catalogue of eight entitlements split into three sections: (1) information and access to personal data, (2) rectification and erasure, and (3) the right to object and automated individual decision-making. The dichotomy between consent and data subject rights fits well within the different stages in our data processing timeline (see Fig. 1 above). In the first stage, the right to information is a key source of control, preparing a data subject for the data processing and its consequences. The right to information is closely tied to consent, since consent is only valid if it is informed, i.e., if the individual receives all the necessary information to approve or disapprove data processing. Consent facilitates control in the second stage of data processing, as it means yes or no for subsequent data processing. In the third stage, "control rights" are of particular importance, because they can ensure control over personal data also in the later stages of data processing (for instance, when data is reused by third parties).

The following sections will explain how the characteristics of human cognitive processing and decision-making form a problem for individuals to gain control over their personal data in the contemporary data-economy. Subsequently, it is discussed how the GDPR aims to address these pitfalls, and what this means in terms of actually enhancing individual control from a behavioural perspective.

Threats to Individual Control in the Information Receiving Stage

Information Overload

A pre-requisite for data subjects' control is being informed about data processing. In order to be in control, a data subject should be able to make decisions that are in line with her existing attitudes and preferences[4] or should at least be aware of what the processing of data entails. In order to do this, the individual requires information. In the *information receiving* stage, data collectors may provide the individual with this kind of information by means of a data use policy. In what follows, we argue that maintaining individual control is not realistic when controlling it is supposed to be provided by means of such information.

Difficulties in cognitively processing information about data collection are an evident threat to individual control. It is important to mention that these difficulties are not only the result of possible cognitive deficiencies within the individual, such as illiteracy, but are inherently related to the contemporary online environment. On a daily basis, individuals are confronted with massive amounts of information divided over different devices, media, and services. This wealth–or rather, overload–of information poses a threat to individuals' ability and motivation to scrutinise the key details that are necessary to make informed privacy decisions.

[3] Other possible types of processing are for example a contract, a controller's legitimate interest, a vital interest of an individual and a public interest. See Article 6 of the GDPR.

[4] However, a side note must be made that these existing attitudes and preferences may also be the result of cognitive processes, wherein an individual was not "in control" of information (see for instance, Chartrand 2005).

Table 1 Threats to individual control in the context of the data economy

	Stage 1 information receiving stage	Stage 2 approval and primary use stage	Stage 3 secondary uses of data (reuse) stage
Cognitive processing and decision-making pitfalls that threaten individual control	Information complexity and literacy Information overload Information asymmetry	Context and choice architecture	Data Affordances: Intangibility Invisibility Scope Flow
Legal provisions in the GDPR addressing these threats to individual control	Information notices Icons	Consent requirements Default settings	Data subject rights: Right to data access and portability Right to erasure

Information processing and decision-making pitfalls that form a threat to control in each of the three data processing stages. Below, the provisions that (aim to) address these threats to control are mentioned

Paradoxically, the more information individuals have access to about what happens to their (personal) data, the less information they are able to filter, process, and weigh to make decisions that are in line with their own privacy preferences.

Yet, when it comes to privacy and data protection mechanisms, such as disclosures, policies, and standard forms, parties that provide the information, including regulators, assume that consumers (are able to) process information extensively. Because of the fast development of technology, such disclosures become increasingly longer and more complex (Shore and Steinman 2015), which puts a growing strain on individuals' cognitive functioning. On top of this, policies often change and, whenever this happens, individuals should read them once again to learn about implications for their personal data. This makes it even more difficult to make informed decisions on personal data disclosure.

In order to make informed decisions, individuals should estimate the expected benefits and sacrifices that are associated with data disclosure and, subsequently, decide whether these are in line with their attitudes and preferences. This would only be possible by first taking into account all information that is made available in these policies, then estimating the consequences of their own data disclosure and the probabilities thereof, and finally by deciding to what extent these consequences (being both positive and negative) are in line with one's own attitudes and preferences. To illustrate the extensive cognitive processing that is required for rational decision-making, in 2016, a Norwegian campaign-group established that it took almost 32 hours to read the terms and conditions of 33 representative smartphone apps (the average number of apps that Norwegians have on their phones; Palazzo 2016). Note that this was solely the time it took to *read* the texts, let alone reflecting on the consequences of agreement to such policies.

Information Complexity

Although limitations in general cognitive abilities may determine how well we are able to read privacy-related information, different levels of specific expertise or "literacy" may play a role as well (Hargittai 2007). Park (2013) examined consumers' literacy with regard to general data policy understanding and found that people correctly answered less than two out of seven questions with regard to their informational privacy (e.g., "A website is legally allowed to share information about you with affiliates without telling you the names of the affiliates").

Jensen and Potts (2004) analyzed 64 privacy policies of US companies (e.g., Google, Weather Channel, eBay) and determined their level of readability by using the Flesch Reading Ease Score. They found that only 6% of them were sufficiently accessible to the Internet population with a high school education or lower. Fifty-four per cent of policies were beyond the grasp of the internet population with more than 14 years of education, and 13% of policies were still beyond the grasp of the internet population with a postgraduate education. These results indicate that a large part of the population–including the higher educated–cannot be expected to understand a substantial number of privacy policies.

Our already restricted information processing capabilities have never been subjected to greater pressure than in the contemporary web environment. Today, data is being processed by using sophisticated artificial intelligence such as algorithms that are not easily explainable (or not explainable at all). The mechanism of data processing resembles a black box–its operation remains largely unknown and the outcomes that follow are unpredictable (Pasquale 2015). The information is presented in such an abstract manner that it is unknown to the individual who receives her data. This results in information asymmetries between the individual and the data collector. What is more, often data controllers themselves do not have knowledge either on who eventually received the data. The consequence is a severe breakdown of informational control.

How Does the GDPR Address These Threats in the Information Receiving Stage?

The Right to Explanation

The GDPR provides three articles on information provision that aim to enhance individual control in this stage, namely the right to explanation.

Before any processing of personal data takes place, a data subject has to be informed, among others, about the purposes for which data will be processed, about the data controller's identity, about the recipients of his personal data and about the period of data storage (Article 13 and 14 of the GDPR). In addition, under the GDPR, a data controller should also provide the information about "… the existence of automated decision making, including profiling […] and at least in those cases, meaningful information about the logic involved as well as the significance and the envisaged consequence" (p. 42)[5]. This new notification duty has received quite some attention both in the media and in academia. To describe its explanatory significance, Goodman and Flaxman coined the expression "the right to explanation" (of the automated decision-making; Goodman and Flaxman 2016). For example, automated decision-making can be used in the recruitment process. Today, recruiters widely use LinkedIn's search tool that automatically selects candidates who will be invited to a job interview. Such automated decisions may significantly affect individuals. Therefore, it is important that data subjects, i.e., prospective job candidates, are properly informed about it. Unfortunately, the GDPR is not very explicit with regard to how specific this explanation should be and its boundaries are still a matter of a fierce academic discussion (e.g., Edwards and Veale 2017; Wachter et al. 2017).

[5] Article 15 of the GDPR.

In the first stage, understanding information is what leads to more control. If someone is aware of data processing and related decision-making, and is able to understand its consequences, this puts her in control over personal data processing. However, in the big data age, algorithmic decisions are increasingly difficult to explain and to comprehend. Arguably, the GDPR gives a right to explanation of algorithms, but this is only an *ex ante* right to explanation rather than *ex post*. In practice, *ex post* explanation would mean that a data subject would be informed about the logic and individual circumstances of their specific decision, the data or features that were considered in her particular case, and their weighting within the decision tree or classification structure. However, according to some scholars the GDPR gives little basis for individuals to claim this sort of explanation (Wachter et al. 2017). What the GDPR only seems to guarantee is an *ex ante* explanation that merely refers to system functionality. For example, in making a decision on credit score, this would include the explanation of general logic (types of data and features considered, categories in the decision tree), purpose or significance (to assign a credit score), and envisaged consequences (the credit score can be used by lenders to assess credit worthiness, affecting the terms of credit such as interest rate).

As it clearly follows, this second, *ex ante* type of explanation does not include the explanation of a specific, individual decision. Obviously, this does not solve the problem of information asymmetries in disadvantage of the data subject. Furthermore, it has been demonstrated that the use of less concrete explanations results in greater information processing difficulties, such as decreased language comprehension and information recall (Holmes and Langford 1976). For this reason, *ex ante* explanation is not particularly successful in solving the problem of information complexity. Nevertheless, the right to explanation should be seen as an improvement, because it is probably the first provision that directly addresses the type of data processing that is among the most invisible; thus, it mitigates threats to individual control that come as a consequence of data affordances.

Icons

The GDPR does not specify how data controllers should fulfil their notification duty, or in other words, how the right to information should be guaranteed. In the context of Web 2.0, the information is usually provided in the web-service's general terms and conditions, or in the privacy policy of the providers' websites (Kosta 2013). As discussed in the previous section, due to the length and complexity of privacy policies, data subjects rarely read them and do not understand them and if they do, they are not capable of following all the changes that frequently occur. The problem is exacerbated on mobile sites where reading long policies is impractical (Edwards and Abel 2014). One possible response to the failure of privacy policies is visualisation by the use of icons. Icons are standardized images that convey key information about data processing. They could be control-enhancing for two reasons in particular: First, they simplify understanding of the information. Second, they save readers' time. The idea has been explicated in the GDPR's article 12(7) which contains the option of using standardized icons stating that "… information […] may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing (L 119/40)." Recital 58 adds that such visualisation should be used "where appropriate" (L 119/11). More detailed guidelines on icons will be prepared by the European Commission (EC) once the GDPR enters in force. It is likely that the EC will rely on the sketch of privacy icons, provided in one of the interim versions of the GDPR (Edwards and Abel 2014).

How effective are icons in enhancing individual control? To solve the problems of information overload, lack of sufficient time and attention devoted to privacy related information, and lack of digital literacy, icons may fulfil a key role. We argue that that icons have the potential to address all three problems related to the provision of information. First, they dramatically reduce the information overload that consumers deal with in the contemporary online environment. Much related to this, they decrease information complexity which strengthens informational control over data processing. As a result, less time and attention is necessary for consumers to grasp the implications of the disclosure of their personal data. Especially standardized icons could play a role in diminishing the problems that arise with regard to the effects of non-standard cues or private logos that may unjustly signal trustworthiness of websites (Hoofnagle and Urban 2014). By providing consumers with and informing them about an international standard for icons that clearly communicate risks that are associated with the disclosure of personal data, consumers may become less reliant on such trivial cues or signals.

However, icons do not provide comprehensive knowledge about data collection practices. In contrast, they only provide information in a manner that is very generalized and simplistic. By using a standardized language that signals trust, consumers may be less susceptible to the fact that they only receive partial information. In the data economy, it is the hidden and intangible details that carry significance rather than some general information (Nissenbaum 2011). That means that by focusing too much on providing easy-to-understand information, icons could actually increase the problem of data invisibility and intangibility. Related to this, if icons ought to protect consumers against hidden purposes of data processing, it is crucial who designs them and with what purposes. The party who designs the icons will obviously be also in control of the responses that these icons will elicit among data subjects. Thus, the risks of using standardized icons should be considered carefully so that they can be implemented in a way that benefits comprehension of data usage instead of merely lowering privacy concerns.

Threats to Individual Control at the Approval and Primary Use Stage

This section addresses the context wherein consent to data collection and processing is requested and affects decision-making. Specifically, it discusses how subtle changes in the context wherein consent is requested and can unconsciously nudge consumers into making decisions that harm their privacy. Finally, it is explained how this relates to a decreased state of control.

In the data-driven economy, parties that provide consumers with privacy information often appeal to the intuitive information-processing mode of consumers. Specifically, it has been demonstrated that subtle differences in choice architecture, such as default settings, can be used to activate or suppress privacy concerns, or even unconsciously steer behaviour–a phenomenon that has been coined “the malleability of privacy preferences” (Acquisti et al. 2015). Because data collectors have an economic interest in disclosure of personal information by consumers, contextual factors that increase disclosure behaviour are attractive for them. Because those interface factors often work in favour of data disclosure outside of voluntary control, it puts the consumer in a vulnerable position (Calo 2013).

One of the most known and perhaps powerful tools to influence privacy preferences is the use of defaults. It has been demonstrated that, when presented with several choice options, consumers generally prefer and choose the option that is marked as the default. This effect

occurs within a wide variety of topics, even in the case of high-involvement issues such as organ donation (Johnson and Goldstein 2003). The effect has also been demonstrated within the field of (personal) data disclosure. For instance, a study by Johnson et al. (2002) indicated that the number of participants who disclosed their personal e-mail address for research purposes increased with 50% when disclosure was the default option. Although these types of effects could intuitively be explained by the possibility that consumers do not read disclosures or are merely indifferent towards them, research has indicated that defaults "work" because of other reasons. For instance, it has been demonstrated that defaults work because they are often (unconsciously) interpreted as recommendations, because people show an unconscious bias towards the status quo (McKenzie et al. 2006), and because individuals have more difficulties in rejecting an option when it is the default due to aversion to "loss" (Smith et al. 2013). These effects become even stronger when consumers process information in the intuitive processing mode. These findings indicate that choice architecture is effective in steering individuals towards certain decisions because they appeal to automatic and intuitive cognitive processes. Importantly for our argument, because of the automatic and intuitive character of these cognitive processes, there is less control over the decision process. That is, while providing consent by changing a default setting (i.e., opt-in) requires that the individual engages in a conscious, affirmative action and hence exerts a form of control, this is not the case when accepting settings as they are. Therefore, privacy invasive default settings can hardly result in individual control over data.

Besides affecting control during decision-making (i.e., by means of choice architecture), the use of contextual cues also affects *subjective experiences* of control. Specifically, the use of contextual cues can also affect the extent to which individuals *perceive* control. For instance, when individuals are made to believe that they have control over their personal information by placing signals that are suggestive of control, they end up disclosing more personal information. For instance, Brandimarte et al. (2013) demonstrated that increasing individual' perceived, but not actual control over the release of and access to their private information, increases their willingness to disclose sensitive information and to a broader audience. Furthermore, a study by Hoofnagle and Urban (2014) found that 62% of respondents to a survey believed that merely the existence of a privacy policy on a website implied that this website was not allowed to share their personal information without permission. It is likely that contextual cues that signal control, such as the mere existence of a privacy policy, implicitly signal trustworthiness, which in turn decreases privacy concerns and increases disclosure behaviour. These findings clearly indicate that communicating to individuals that they are in control is not enough to enhance actual control–in some cases, it may wrongfully signal trustworthiness and decrease privacy concerns in turn. It should be noted that communicating control to individuals by means of choice architecture and design should always go together with a situation that actually enhances control, such as data protective defaults.

In conclusion, the use of contextual cues and choice architecture relates to individual control in several ways. First, subtle cues are effective in altering privacy preferences by making use of bounded rationality. Hence, these factors change privacy preferences especially when people engage in intuitive, uncontrolled information processing and thus exploit the lack of individual control. Second, contextual cues are able to increase or decrease *perceived* control. This may in turn result in (false) perceptions of either trust or distrust, and increased or decreased privacy concerns.

How Does the GDPR Address These Threats at the Approval and Primary Use Stage?

Consent is subject to additional conditions under the GDPR. A valid consent presupposes that a data subject has fully understood the consequences of his or her approval. In Article 4 of the GDPR, consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (p. 34). What this may mean in practical terms is indicated in Recital 32, which states that unambiguous consent may be signified by ticking a box or by making a statement that clearly indicates acceptance of data processing for the specific purpose of processing at hand. Further, the (non-binding) Recital 32 indicates that "silence, pre-ticked boxes or inactivity should not therefore constitute consent (p. 6)." Due to the prohibition of silence, pre-ticked boxes or inactivity as a basis for consent under the GDPR, individuals are granted more control over their data. That is, in terms of the cognitive processes that play a role in decisions about consent, the requirement that consent should be active and should not rely on silence, inactivity, or pre-ticked boxes increases the extent to which the act of consenting is voluntary and hence under control of the individual.

Consent may also be given through "another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data" (p. 6, Recital 32). This means that consent is also possible without an explicit agreement to data collection. Consider an individual who visits a website where she fills out a form with her name and address information to participate in, for instance, an online competition. When a short disclaimer is visible on the website that reads "enter your e-mail address to receive special offers," the individual will provide lawful consent by typing in her e-mail address. Note that under the GDPR, "unambiguous consent" is different from "explicit consent," which is described in Article 9 of the GDPR and applies to "sensitive" types of data, such as ethnic origin, political opinions, and sexual orientation. The principle of explicit consent *does* require that the individual makes or confirms a specific statement such as "I consent to (..)" In the initial Commission's proposal for the regulation (Interinstitutional File 2012), there was called for explicit consent in all cases, not just in cases that concerned sensitive data. In the final version of the regulation, a distinction was made between unambiguous consent (ordinary data) versus explicit consent (sensitive data). Unfortunately, compared to unambiguous consent, explicit consent would have substantially increased individual control over personal data.

Next to prohibiting pre-ticked boxes (i.e., opt-out) as consent, the GDPR embeds the more general "privacy by default" principle in Article 25, where it states: "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.[…] In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons" (p. 48). Thus, by default, only personal data that are necessary for a specific stated purpose of processing are processed. In a social network environment for instance, this would mean that users' profiles would not be public unless a user explicitly changes the settings.

Further, note that these requirements only apply when consent is the only legal basis for lawful processing of data. When relying on other principles as the basis for lawful processing, such as a contract, compliance with a legal obligation, or the public interest, the controller is not required to implement these changes.

Control at the Data Reuse Stage

In the modern data economy, personal data is not only used once. Rather, it is widely shared, reused and oftentimes misused. A compelling example of data misuse is the case of Cambridge Analytica, the company that used personal information of millions of U.S. Facebook users without authorization, and used this information to profile and target users with personalized political advertisements. Not only did the scandal result in the bankruptcy of Cambridge Analytica, it also resulted in a 500,000 Dollar fine for Facebook for its part in the scandal. The Information Commissioner's Office (ICO) concluded that Facebook had failed to safeguard its users' information and that it failed to be transparent about how that data was harvested by other parties than Facebook itself (The Guardian 2018).

Looking at these trends, threats to individual control over personal data increasingly emerge in the third stage. Even though the reasons for collection of data may be straightforward (e.g., subscribing to an online service; using a social media platform) and data processing initially seems under control, its secondary uses may be very opaque (e.g., sharing users' data with data brokers) and thus control starts decreasing.

Besides the problems that arise with regard to the processing of information and the misleading effects of context and choice architecture, the characteristics of data itself also pose threats to individual control. That is, affordances of generated personal data in terms of its *intangibility*, *invisibility*, and *scope and flow* restrict individual control in the reuse stage. As will be apparent below, these concepts overlap with each other to a certain extent. Further, although these affordances are affecting control from the moment that the data is released (after the point of approval), they particularly pose a threat to control in this third stage of our data processing timeline, when data spread throughout the digital environment.

Personal data are, unlike tradable goods, physically intangible. It is harder to experience control over something that cannot be literally held or touched (Kamleitner and Mitchell 2018). It has been demonstrated that people ascribe a higher value to the same objects when these are physical, as opposed to digital (i.e., photos, books), and identify themselves more with these objects in terms of psychological ownership (Atasoy and Morewedge 2017). Furthermore, the intangible aspect of personal data enables duplication and sharing of data. Not being able to grasp the exact quantity and "locations" of data points makes it difficult to exercise control over these data.

Closely related to the intangibility of data is its invisibility. To consumers, the personal data that are being collected by parties are permanently invisible, especially when it comes to behavioural data. Although consumers are in many cases allowed to gain insight in the specific personal data that have been collected by companies, the generally invisible character of online processed personal data may prevent consumers from seeking out insight into these data in the first place. Making personal data more visible, for instance by providing visual designs that make personal data more comprehensive, may help consumers in understanding what is happening and will make them feel more in control (Niezen et al. 2010; Kamleitner and Mitchell 2018).

Finally, after data has been collected, it is processed and, in the third stage, it flows to third party data processors or to new controllers. Here, databases may be restructured and merged with other databases that are acquired via additional parties. For instance, to enrich data that is provided or generated by users, platforms acquire additional personal data by collaborating with data brokers or using of open source data. The route that personal data takes can be very opaque and complex. Not only individuals but also data collectors and data processors are

often ignorant with regard to the parties that eventually receive data given piece of data. Therefore, in terms of the scope and flow of data streams, individual control is certainly challenged.

How Does the GDPR Address Threats to Control at the Data (Re)Use Stage?

As mentioned above, control rights as defined in the GDPR are of particular importance for individuals, because they can ensure control over personal data also in the later stages of data processing.[6] Control rights that particularly aim to increase individual control are the right to data portability, the right to access and the right to erasure. Within the scope of this paper, special attention is being paid to the right to data portability.

Right to (Data Access and) Portability

The right to data portability (Article 20 of the GDPR) is of special relevance as it is new to the fabric of personal data protection (Irion and Luchetta 2013). The wording of the provision suggests that the right is split into two elements. First, the data subject has the right to obtain "a copy of the personal data undergoing processing" (i.e., the right to access, p. 45). This copy must be provided free of charge. This right to access is intended to allow individuals to check whether the processing of their data is lawful. The controller should provide the purpose of processing, the categories of processed data, and–new in the GDPR–the (categories of) recipients, the envisaged retention period, the right to rectification and erasure, information about how the data is acquired, and whether there was automatic decision-making involved. Further, as stated in (the non-binding) Recital 63, the controller may provide a secure system that would provide the data subject with access to the data. Second, individuals have the right to transmit their personal data from one provider to another.[7] The basic idea of this right is that an individual would be able to transfer his or her personal data and other material from one information service, say Facebook, to another, say Google+, without hindrance (Swire and Lagos 2012). Until now, these types of industries appear prone to monopolisation, whether as a result of innovation, network effects, or even acquisitions, which jeopardizes individual control over personal data–individuals simply have no choice (Lynskey 2015). It is believed that portability could enable individuals to maximise the advantages of big data and to benefit from the value created by the use of their personal data. For example, it would allow them to use the data for their own purposes, or to share data with third parties, in exchange for their services (European Data Protection Supervisor 2015).

As expressly acknowledged in the GDPR (Recital 68), data portability's main goal is "to strengthen [data subject's] control over his or her data" (p. 13). Notably, by applying the portability right that individuals are able to influence how their data is not only used but also *re*used. To some extent, the right to data access and portability could solve the problem of control in terms of increased invisibility and clarification of the scope of data streams. That is, by providing consumers with a digital copy of the data they disclose, visibility of data could be

[6] It has to be noted that withdrawal of consent can also be effective in later stages of data processing.
[7] In the amended text of the European Parliament, both aspects are joined in the same section of the article on the right to access, namely Article 15(2)(a).

increased. Providing consumers with online platforms on which they could transmit their data from one party to another would further help to visualise their data and hence help to solve the problem of data invisibility. As also posed by Kamleitner and Mitchell (2018), visualizing data streams could be helpful in increasing consumer understanding about what happens to data after consent is initially given.

However, the provision has two important drawbacks. First, not all personal data can be made portable. Under Article 20, only data that a data subject has provided by herself fall under the definition of portable data. Observed data such as location tracking is left out of the scope (Meyer 2017[8]). Being intangible and invisible, observed data is a typical representative of control-weakening data affordances. As it can be nevertheless very much privacy revealing, it would certainly benefit from increased consumer control. Unfortunately, the right to data portability is not helpful in this regard. Second, data portability allows individuals to receive and transmit their data but it does not automatically mean that the data is removed from the original location and deleted. For this to occur, an additional request for deletion is necessary. The right to portability may give an impression that collected data can be transferred as physical objects, while in fact, the right only applies to an electronic copy of a data set.

The Right to Erasure

Article 17 states that, in situations wherein data processing does not satisfy the requirements of the GDPR, processing may be considered as *unlawful* and data subjects have the right to have their data erased. This may be the case when, for instance, data are no longer necessary for the purpose for which they were initially collected and processed, or simply when the individual withdraws consent to processing. An important obligation of the data controller is that in the case of data erasure, the controller must notify any one to whom data have been disclosed, unless this would be impossible or involve disproportionate effort.

The right to erasure may address the negative consequences of the intangibility of data. As noted before, because of its intangibility, personal data in principle has the characteristic that it can be multiplied almost unlimitedly. The right to data erasure, and especially the obligation of the data controller to notify other parties of data erasure responsibilities, increases individual control of the scope and flow of these data. Individuals did not use to have any substantial control over the scope and flow of their data once it spread throughout the digital environment in the third stage of data processing. Under the GDPR, individuals have more control in terms of the scope and flow of their data in situations where data processing is unlawful and the right to erasure applies.

However, it is unclear under what conditions data processing can be considered as unlawful. The implementation of the GDPR's right to erasure by the Member States is still dependent on the Member States' drafted exemptions. For instance, erasure is not obligated when data erasure would be associated with disproportionate effort.

Conclusion and Discussion

The General Data Protection Regulation emphasises the importance of enhancing individual control in the data economy. In this paper, we have analysed a number of relevant

[8] Although Article 29 Working Party included observed data in their definition of portable data, the EU authorities dismantled this interpretation.

provisions in this regulation and have determined the extent to which they enhance individual control over consent-based data processing. In particular, we have examined how the provisions address threats to individual control that are increasingly present in the data economy and that appear in the three stages of the data processing timeline: (1) the information receiving stage, (2) the approval and primary use stage, and (3) the data secondary use (reuse) stage. By analysing the threats to individual control from a behavioural perspective, we have provided a perspective on the effectiveness of the GDPR in enhancing individual control.

In the information receiving stage, the new right to explanation has the potential to address the problem of data affordances, making automated decisions more visible. However, it fails to solve the problem of information complexity, as it only provides general (ex-ante) explanation of automated decision-making and does not explain what are actual implications for an individual. Icons could be more successful in mitigating information complexity, but there is a risk that they may worsen the problem of biases in decision making, since they only provide a partial description of the data processing.

In the approval and primary use stage, the new principle of privacy by default and the increased requirements with regard to consent increase individual control substantially by requiring affirmative action before data is being collected. Consent should be given unambiguously, and a positive indication of agreement with data collection is necessary to provide lawful consent-based processing. However, although Recital 32 indicates that silence, pre-ticked boxes or inactivity should not constitute consent, it is unclear how this non-binding recital shall be implemented by the member states. For privacy by default to be successful in enhancing individual control, it is crucial that it is implemented in a way that it indeed empowers individuals.

In the data reuse stage, the right to access and portability gives control to individuals but only over a very limited scope of personal data. Observed data such as location data that can be very much privacy revealing fall out of scope. Still, the right to portability may decrease invisibility of data in combination with the use of electronic data platforms where individuals are able to manage their own data. It is still to be seen whether such platforms will emerge on a larger scale in the future, but they will most likely help in visualising the scope and flow of one's data. Moreover, we conclude that individuals have more control in terms of the scope and flow of their data in situations where data processing is unlawful and the right to erasure applies.

Our analysis points out that from a behavioural perspective the GDPR took important steps in addressing threats to individual control. As a comparison, the former data protection directive had almost no reference to individual control. However, as the GDPR is still open at some points (member states can decide to implement or interpret it in different ways), it is important that the pitfalls in human decision-making are carefully considered in future development of the implementation of this regulation.

This work provides an aid in exposing and addressing the problems that arise with regard to individual control in the data-driven economy. We have argued that several provisions in the GDPR serve as helpful steps in enhancing individual control. Moreover, some of the deficiencies that remain entrenched in the GDPR may be mitigated by self-regulatory instruments, such as code of conducts or the EC delegated acts, as foreseen in the GDPR. As these instruments unfold, it remains critical that lawyers, policy makers and behavioural scientists keep cooperating to improve the effectiveness of future data protection law in terms of protecting consumer rights. Although the primary aim of this

work is not to provide specific solutions to the problem of declining individual control, we hope to have sparked a discussion that stimulates such cooperation and helps addressing the pressing problem of weakening individual control in the data-driven economy.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514.

Atasoy, O., & Morewedge, C. K. (2017). Digital goods are valued less than physical goods. *Journal of Consumer Research, 44*(6), 1343–1357.

Bargh, J. A. (1994). The four horsemen of automaticity: Awareness, intention, efficiency, and control. In R. Wyer & T. Srull (Eds.), *Social cognition. Handbook of social cognition* (pp. 1–40). London: Psychology Press.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340–347.

Bundesverfassungsgericht, U. V. (1983). 15. Dezember 1983 zum Volkszählungsgesetz 1983. *Bundesanzeiger 35241a*. Retrieved from https://freiheitsfoo.de/files/2013/10/Census-Act.pdf. Accessed 4 Dec 2018.

Calo, R. (2013). Digital market manipulation. *George Washington Law Review, 82*, 995–1051.

Cohen, J. E. (2018). Turning privacy inside out. *Theoretical inquiries in law.* (forthcoming 2019).

Chartrand, T. L. (2005). The role of conscious awareness in consumer behavior. *Journal of Consumer Psychology, 15*(3), 203–210.

Custers, B., van Der Hof, S., Schermer, B., Appleby-Arnold, S., & Brockdorff, N. (2013). Informed consent in social media use-the gap between user expectations and EU personal data protection law. *SCRIPTed, 10*, 435–457.

Edwards, L., & Abel, W. (2014). *The use of privacy icons and standard contract terms for generating consumer trust and confidence in digital services*. CREATe working paper series. Retrieved from https://www.create.ac.uk/publications/the-use-of-privacy-icons-and-standard-contract-terms-for-generating-consumer-trust-and-confidence-in-digital-services/. Accessed 28 Nov 2018.

Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. *Duke Law and Technology Review, 16*(1), 1–65.

European Data Protection Supervisor. (2015). *Annual Report*. European Union. Retrieved from https://edps.europa.eu/sites/edp/files/publication/edps_annual_report_2015_web_en.pdf. Accessed 28 Nov 2018.

Interinstitutional File. (2012). *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)*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52012PC0011. Accessed 28 Nov 2018.

G. D. P. Regulation (GDPR) (2016). Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46. *Official Journal of the European Union, 59*, 1–88.

Goodman, B., & Flaxman, S. (2016). *European Union regulations on algorithmic decision-making and a" right to explanation*" (1606.08813). ArXiv. Retrieved from https://arxiv.org/abs/1606.08813. Accessed 28 Nov 2018.

Hargittai, E. (2007). Whose space? Differences among users and non-users of social network sites. *Journal of Computer-Mediated Communication, 13*(1), 276–297.

Holmes, V. T., & Langford, J. (1976). Comprehension and recall of abstract and concrete sentences. *Journal of Verbal Learning and Verbal Behavior, 15*(5), 559–566.
Hoofnagle, C. J., & Urban, J. M. (2014). Alan Westin's privacy homo economicus. *Wake Forest Law Review, 49*, 261.
Irion, K., Luchetta, G. (2013). CEPS task force report of the CEPS digital forum. Resource Document. Centre for European Policy Studies. Retrieved from https://ssrn.com/abstract=2275267. Accessed 28 Nov 2018.
Jensen, C., Potts, C. (2004). Privacy policies as decision-making tools: An evaluation of online privacy notices. In K. Dykstra-Erickson, M. Tsscheligi (Eds.), *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 471–478). ACM.
Johnson, E. J., Bellman, S., & Lohse, G. L. (2002). Defaults, framing and privacy: Why opting in-opting out. *Marketing Letters, 13*(1), 5–16.
Johnson, E. J., & Goldstein, D. (2003). Do defaults save lives? *Science, 302*(5649), 1338–1340.
Kamleitner, B., & Mitchell, V. W. (2018). Can consumers experience ownership for their personal data? From issues of scope and invisibility to agents handling our digital blueprints. In J. Peck & S. Shu (Eds.), *Psychological ownership and consumer behavior* (pp. 91–118). Cham: Springer.
Koops, B. J., Newell, B. C., Timan, T., Skorvanek, I., Chokrevski, T., & Galic, M. (2016). A typology of privacy. *University of Pennsylvania Journal of International Law Review, 38*, 483.
Kosta, E. (2013). *Consent in European data protection law*. Leiden: Martinus Nijhoff Publishers.
Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford: Oxford University Press.
Mantelero, A. (2013). The EU proposal for a general data protection regulation and the roots of the 'right to be forgotten. *Computer Law and Security Review, 29*(3), 229–235.
Mantelero, A. (2014). The future of consumer data protection in the EU re-thinking the "notice and consent" paradigm in the new era of predictive analytics. *Computer Law and Security Review, 30*(6), 643–660.
Meyer, D. (2017). European Commission, experts uneasy over WP29 data portability interpretation. *The Privacy Advisor*. Retrieved from https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/. Accessed 28 Nov 2018.
McKenzie, C. R., Liersch, M. J., & Finkelstein, S. R. (2006). Recommendations implicit in policy defaults. *Psychological Science, 17*(5), 414–420.
Niezen, G., van der Vlist, B. J. J., Hu, J., & Feijs, L. M. G. (2010). From events to goals: Supporting semantic interaction in smart environments. In *Proceedings of the Computers and Communications (ISCC), 2010 IEEE Symposium on Computers and Communications* (pp. 1029–1034).
Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*, 119.
Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, 140*(4), 32–48.
Palazzo, C. (2016). Consumer campaigners read terms and conditions of their mobile phone apps. all 250,00 words. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/technology/2016/05/26/consumer-campaigners-read-terms-and-conditions-of-their-mobile-p/. Accessed 28 Nov 2018.
Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215–236.
Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge, MA: Harvard University Press.
Reding, V. (2011). *Your data, your rights: Safeguarding your privacy in a connected world.* Keynote at World Privacy Platform "The review of the EU data protection framework", Brussels. Retrieved from https://europa.eu/rapid/press-release_SPEECH-11-183_en.pdf. Accessed 28 Nov 2018.
Shore, J. & Steinman, J. (2015). Did you really agree to that? The evolution of facebook's privacy policy 2015. Resource document. *Technology Science.* Retrieved from https://techscience.org/a/2015081102. Accessed 28 Nov 2018.
Smith, N. C., Goldstein, D. G., & Johnson, E. J. (2013). Choice without awareness: Ethical and policy implications of defaults. *Journal of Public Policy & Marketing, 32*(2), 159–172.
Solove, D. J. (2007). *The future of reputation: Gossip, rumor, and privacy on the internet*. New Haven: Yale University Press.
Swire, P., & Lagos, Y. (2012). Why the right to data portability likely reduces consumer welfare: Antitrust and privacy critique. *Maryland Law Review, 72*, 335–380.
The Guardian. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian.* Retrieved from: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Accessed 28 Nov 2018.
Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law, 7*(2), 76–99.
Westin, A. F. (1968). *Privacy and freedom*. New York: Athenum.

Affiliations

I. van Ooijen [1] · Helena U. Vrabec [2,3]

Helena U. Vrabec
ursic.h@law.leideuniv.nl

[1] Department of Communication Science, Faculty of Behavioural, Management and Social Sciences, Twente University, Building Cubicus, P.O. Box 217, 7500 AE Enschede, the Netherlands

[2] Yale University, New Haven, CT, USA

[3] Leiden University, Steenschuur 25, 2311 ES Leiden, the Netherlands