

The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection

Benjamin Bergemann

► **To cite this version:**

Benjamin Bergemann. The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection. Marit Hansen; Eleni Kosta; Igor Nai-Fovino; Simone Fischer-Hübner. Privacy and Identity Management. The Smart Revolution: 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Ispra, Italy, September 4-8, 2017, Revised Selected Papers, AICT-526, Springer International Publishing, pp.111-131, 2018, IFIP Advances in Information and Communication Technology, 978-3-319-92924-8. 10.1007/978-3-319-92925-5_8. hal-01883620

HAL Id: hal-01883620

<https://hal.inria.fr/hal-01883620>

Submitted on 28 Sep 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection

Benjamin Bergemann

WZB Berlin Social Science Center, Berlin, Germany

benjamin.bergemann@wzb.eu

Abstract. The concept of consent is a central pillar of data protection. It features prominently in research, regulation, and public debates on the subject, in spite of the wide-ranging criticisms that have been levelled against it. In this paper, I refer to this as the consent paradox. I argue that consent continues to play a central role not despite but because the criticisms of it. I analyze the debate on consent in the scholarly literature in general, and among German data protection professionals in particular, showing that it is a focus on the informed individual that keeps the concept of consent in place. Critiques of consent based on the notion of “informedness” reinforce the centrality of consent rather than calling it into question. They allude to a market view that foregrounds individual choice. Yet, the idea of a data market obscures more fundamental objections to consent, namely the individual’s dependency on data controllers’ services that renders the assumption of free choice a fiction.

Keywords: Commodification · Data protection · Discourse analysis · Informed consent · Information control · Power.

1 Introduction: The Consent Paradox¹

Despite criticism, consent enjoys a massive and ongoing presence in data protection. I refer to this counterintuitive observation as the *consent paradox*. Consent is omnipresent in policy making, regulatory practice, and scholarly debates. Yet, the prominent role ascribed to consent in data protection is puzzling given the sustained critique from data protection professionals and average users alike [2, p. 171]. Both groups argue that it is hard for users to comprehend what they are consenting to. Moreover, they criticize that users often do not have a choice but to consent because they rely on products such as social network services or smartphones. In data protection parlance, lay people and specialists criticize that consent is, in many cases, neither *informed* nor *freely given*. Nevertheless, consent continues to be an essential part of data protection both in theory and practice. The aim of my paper is to account for this consent paradox: How is it that consent is ascribed such a prominent role in data protection while at the same time being subject to numerous criticisms?

¹ This paper refines several arguments that I have developed in my master’s thesis [1].

I set out to explain the consent paradox in data protection by analyzing the nexus between criticizing consent and keeping it in place. In other words, I assume that the consent paradox does not exist *despite* but *due to* the criticisms of consent. Thus, I do not discuss in how far consent *is* a meaningful instrument of data protection. Instead, I analyze how this very discussion *makes* consent a fitting solution to today's data protection problems. At first glance, assuming a productive, rather than a destructive relationship between critique and its object appears counter-intuitive. However, the idea is not unfamiliar in political sociology [3, p. 27] and, more importantly, seems to tie in well with others' observations regarding consent in data protection.

Several scholars have repeatedly pointed to what I term a consent paradox. They emphasize that consent continues to be an essential part of data protection policies despite its perceived limits [see 4–6]. Koops, criticizing a “mythology of consent”, wonders why “the conclusion is too seldom drawn that consent is simply not a suitable approach to legitimate data processing in online contexts” [6, p. 251]. For Koops and others the consent paradox is manifested in the new General Data Protection Regulation (GDPR), which, according to them, has a strong focus on consent and individual information control in general [see 7, p. 313].

Some authors have already suggested a connection between criticizing consent and keeping it in place. Zanfir notes that the modifications made to consent in the GDPR “are responses to the critiques of the provisions in the [Data Protection Directive]” [5, p. 241]. Arguing in the same direction, Schermer et al. state that “the crisis of consent” has led to regulatory attempts to reform consent [2, p. 172]. A similar observation has been made by Barocas and Nissenbaum from an US perspective [8, p. 58]. According to them, questioning consent prompts an “urgent need” to fix it. Elaborating further on the nexus between critique and reform, Rouvroy and Poullet suggest that certain kinds of critique can be addressed by reforming consent, while more fundamental objections, resulting from “socio-economic and other structural inequalities,” seem to question consent in general [9, p. 74]. One issue with consent that falls into the former category of perceived ‘solvable’ problems is ensuring that individuals consent in an *informed* manner. As authors on both sides of the Atlantic observe, enhancing individual information provision seems to be the most common suggestion for mitigating the problems with consent [6, p. 252, 7, p. 318, 9, p. 74, 10, p. 5, 11, p. 3].

Yet, the studies mentioned make these observations in the course of other arguments, thus only touching upon the question I want to answer in this paper: How can we account for the prominent position of consent despite critique? To answer this question, I develop these arguments further, proceeding in two steps. I first review the scholarly critiques of consent. In a second step, I complement this literature review by analyzing the debate on consent among German data protection professionals between 2000 and today.

Drawing on this analysis, I claim that it is the emphasis on *informedness* that keeps consent in place. Criticizing consent in terms of information asymmetries makes reforming consent not only a feasible but also a valuable project. As I will show in the following, this is because problematizing consent in terms of information asymmetries goes along with the idea of seeing data protection through a market lens. From

the data market viewpoint, consent is a key instrument for consumers to exchange “their data” in order to benefit from the services provided by internet companies. However, for the consumer to understand that she is benefiting from the transaction of “her data,” it must be clear to her what is in the deal. This ties the data market narrative to the legal requirement of *informed* consent, making it the yard stick for proper consent. The focus on informedness, I argue, comes at the expense of an understanding of data protection in terms of power. Approaching consent from the perspective of power asymmetries calls into question whether consent can be *freely given*, thus challenging the case for consent more profoundly.

My contribution takes a discourse analytical perspective. It differs from most of the literature on consent in that it does not argue from a legal or philosophical standpoint. I try to show how the debate on consent in data protection, although being legal in nature, is shaped by greater societal debates and conflicts. My goal is to map the discussion on consent in data protection, to understand its inner workings and the effects it produces. One such effect, I suspect, is the consent paradox.

The paper is structured as follows. The second part introduces the consent approach in data protection and its respective critiques. Looking at the critical debate about consent as the assumed source of the consent paradox, I argue that a closer, more empirical, view is needed to understand how exactly criticizing consent leads to the consent paradox. Third, I briefly introduce discourse analysis as my methodology. Then I present the debate on consent among German data protection professionals between 2000 and today as my object of analysis, explaining the case selection and the steps taken to come to my findings. The results are presented in section four. In the concluding section, I reflect on the implications of my argument for data protection research and practice.

2 Consent in Data Protection and its Discontents

The aim of this section is to present the basics of the consent debate in data protection and linking it to the idea of the consent paradox. In line with the scope of my paper, this section will focus on the literature about consent in data protection, excluding other important work on the role of consent, most notably in the medical field [12, 13].² As the field of data protection is traditionally dominated by legal scholars [15, p. 76], I often refer to legal scholarship and documents. Yet, I do not provide a legal analysis of consent in data protection.

² Works on consent in the medical field have considerably influenced the academic debate on consent in data protection. Kosta [14] as well as Barocas and Nissenbaum [8] rely on arguments from the literature on consent in the medical field. From a discourse analytical perspective, linking two distinct fields is interesting in its own right. One could ask what implications such an analogy has for data protection and consent, in contrast to borrowing from other analogies such as the rule of law [4].

2.1 The Consent Paradox in European Data Protection Law

Legally speaking, consent is just one of the six legal grounds that authorize the processing of personal data in European data protection legislation [5, p. 237]. This has been true since the 1995 Data Protection Directive (DPD) and has been continued in the new General Data Protection Regulation (GDPR). Here, consent is defined as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her” (art 4). There are other legal grounds to base processing on, most importantly, the performance of a contract, legal provisions and the legitimate interest of the data controller. According to European data protection law, consent also does not change the fact that every data processing, regardless of its legal basis, is “subject to ‘suitable safeguards’” [5, see also 16]. As Zanfir [5] describes, suitable safeguards encompass the principle of purpose limitation, data subject’s rights and organizational and enforcement measures to hold data controllers accountable. In short, consent is always embedded in an environment of other data protection rules and principles. Yet, the degree to which data protection rules should focus on consent—in law as well as in practice—has been disputed among specialists.

The new GDPR, as several authors have noted, keeps with the directive’s emphasis on consent, which is in line with my argument of a consent paradox [5–7, 17]. Yet, Quelle has convincingly argued that consent’s and user control’s role in the GDPR is a matter of interpretation [18].³ What, however, speaks in favor of reading the GDPR in terms of a consent paradox is that it not only keeps with consent, but it does so *through* the process of reforming it. Most of those reforms address the requirements of freely given and informed consent.⁴ The GDPR, in other words, speaks to the criticisms of consent that I will introduce in the paragraphs ahead.

Finally, I do not intend to imply that the GDPR is the only instance of the consent paradox. The preoccupation with consent and its improvement manifests itself in research and development projects, campaigning and litigation activities or privacy literacy efforts, just to name a few. Yet, legal instruments such as the GDPR are especially important since—on the one hand—they are a product of professional and societal debates. On the other hand, they are also a guiding source for new discussions, regarding laws’ interpretation and future reform. To better understand the consent paradox, the following section will turn from one of its empirical manifestations to one of its assumed sources: the critical debate about consent among specialists.

2.2 Consent and its Critics: Neither Freely Given, nor Informed?

Despite its stable and prestigious position in European data protection, consent has faced critique by practitioners and scholars alike. While criticisms of consent are as

³ Lynskey provides an in-depth discussion of data protection law’s understanding of individual information control [19].

⁴ Discussing the reforms made to consent in the GDPR is outside the scope of this paper. They have been described elsewhere [see 17, p. 9, 18, p. 142].

old as consent in data protection itself⁵, the last decade has seen an increasing number of critical engagements with the consent approach, especially in academia. There are different ways to map this vast literature. In line with the previous section, I will concentrate on those accounts that criticize consent regarding the requirements of freely given and informed consent.⁶

Several voices doubt that there are many examples of *freely given consent in practice*. The practice they usually refer to is the use of notice and consent by digital platforms [see 6, p. 251]. Here, they lament, the individual is not free to authorize the processing of her data for three major reasons. First, for the individual there is “little to no room for negotiation” [2, p. 177] as she can only consent to standardized privacy policies [see also 4, p. 143]. She is thus not expressing her free choice. She merely reacts to a “take it or leave it” deal. Second, the data subject often has no choice but to consent since they are no alternatives among the quasi-monopolies of internet platforms, let alone more data protection-friendly ones [6, p. 252]. Third and related, users increasingly depend on the usage of digital platforms [21, p. 297], reflecting the fact that they became private infrastructures, necessary to exist in our digital societies. In sum, all three arguments state that consent does not live up to its promise of free choice due to power imbalances between users and platforms. What sets these criticisms apart from the next line of arguments is that they consider power imbalances as distinct from information asymmetries. This implies that properly informing the data subject will not suffice to redress consent’s shortcomings [see 19, p. 260].

Among those critiques based on the notion of freely given consent, there is a general tendency to raise doubts about the reformability of consent, at least in the narrow sense proposed in the GDPR. Most contributions in this camp advocate, although often rather vaguely, for regulating the behavior of data controllers to ensure the fairness of data processing [2, 4, 6, 21]. Focusing on controllers and their operations, they argue, would allow for reducing the burden the user. More specifically, Koops suggests relying on other legal grounds than consent in “online contexts” [6, p. 252]. Rhoen proposes to address power asymmetries between data subjects and controllers by evaluating “privacy contracts”, by which he means the legal grounds of both consent and contract, with the help of consumer law’s notion of “unfair terms” [22]. He thus advocates to complement the “formal requirements” of data protection law with consumer law, regulating what can fairly be consented to by the consumer in the first place [22]. However, the bigger point among those critics seems to be that the emphasis on consent should be reduced, which speaks against my hypothesis that the consent paradox stems from reforms induced by consent’s critics.

⁵ Tellingly, it was only after a heated debate that the first German data protection act of 1977 included consent as a legal ground for processing personal data. Early adopters of automatic data processing argued that only consent alone could provide for the legal certainty required to implement the new means of data processing. Critics, on the other side, claimed that the consent provision would constitute a potential loophole, allowing data controllers to depart from stricter data protection obligations [20].

⁶ This excludes several serious objections, for instance that, even under perfect conditions, consent cannot ensure privacy and data protection due to the technical possibility of making inferences—even about those who do not disclose their data [7, p. 322, 8, p. 61].

The second, and apparently more common, criticism of consent concerns its *informedness*. Again, I will focus on the three major lines of reasoning in the literature [for comprehensive accounts see 2, 23, 24]. The first critique addresses the fact that most people do not read privacy policies [see 23, p. 1883]. The most often-cited reason for this is that reading privacy policies takes too long (“information overload”) while at the same time there are too much of them (“consent overload”) [2, p. 177]. The objective amount of time that would be needed to read, or even skim, the privacy policies presented to data subjects by far exceeds the time that can be reasonably expected to be invested by the average user [see 2, p. 177]. Schermer et al. argue further that information and consent overload lead to “consent desensitization”, that is, people giving their consent blindly, thereby devaluing consent and lowering the level of data protection in the long term [2, p. 178]. A second line of objections raises doubts over the possibility of understanding privacy policies and data processing more generally. To begin with the latter, modern data processing operations in general are difficult to comprehend for the average data subject and the specialist alike [8, p. 59, 23, p. 1888]. As Solove points out, the same is true for the consequences caused by a lack of privacy/data protection as they often remain “abstract” [23, p. 1885]. Privacy policies, in turn, need to translate these complexities ensuring informed consent.⁷ As a result, privacy policies turn out to be difficult to understand. This is only aggravated by the highly standardized and often legalistic language used in privacy policies [see 23, p. 1884]. The problem with understanding privacy policies is often discussed in terms of a “transparency paradox” as Barocas and Nissenbaum put it [8, p. 58]. While it seems obvious that privacy policies could be simplified to ease the users’ understanding, the loss of complexity necessarily involves a loss of information [see 6, p. 252, 23, p. 1886]. Third and lastly, it is far from clear whether better information also leads to better decisions by data subjects. In fact, people’s decision-making, is “skewed” [23, p. 1886], since it is largely decoupled from the quality of information provided to them. Rather than by information provisions, users are influenced by their own biases and the immediate context of their decisions, for example, what their perceived short-term gains are [see 25, p. 6].

The problem of how to improve the informedness of users has motivated numerous researchers and practitioners. Ideas on how to improve users’ ability to notice, read, understand and decide abound [for an overview see 24]. Most of them involve visualizing (images, icons) as well as simplifying and condensing information into different degrees of complexity. Often, this is combined with rating the privacy policies’ content [24, 26]. Rating can take the forms of warnings (mostly from third-parties) but also comes in more positive forms such as official labels and certificates where the quality of processing conditions is granted by a certification authority [see 24, p. 39].⁸

⁷ For a more general critique on this reduced understanding of how humans process information see Barocas and Nissenbaum [8] who refer to Manson and O’Neill’s *Rethinking informed consent in bioethics* [12]. Manson and O’Neill provide an in-depth discussion of how human information processing works and the consequences of these insights for informed consent.

⁸ Interestingly, procedural and substantial measures overlap in the latter case, situating certification approaches in-between so-called “paternalistic”, that is, organizational measures addressing the behavior of data controllers, and improving user choice.

Others seek to improve the user's informedness by personalizing privacy policies and notices in accordance with her level of knowledge [see 24, p. 44]. Last but not least, with the rise of behavioral research that brought to fore users' irrational decision making, the idea of nudging people into better privacy decisions, for instance through designing applications and small notices in particular ways, has gained credibility in recent years [see 25]. Finally, it is important to note that the literature does not claim that improved information provisions will solve all of consent's problems. Rather, it is regarded as a first step to reform [see 24, p. 62].

Summing up the literature review, it becomes clear that criticizing the informedness of consent is linked to a more profound interest in reforming consent. Thus, criticizing consent in terms of informedness seems to re-emphasize rather than to call into question consent in data protection, which is in line with the consent paradox hypothesis. However, the evidence gained from the scholarly accounts cannot explain the consent paradox satisfactorily. First, while the literature review can provide initial evidence for the consent paradox, it fails to account for the fact that criticizing consent in terms of information asymmetries appears more prominent than the objections regarding power asymmetries. What is it that makes the information camp's arguments so compelling and amenable to the consent discussion? Second, foregrounding either freely given *or* informed consent, the critiques discussed do not explain how to—technically—deal with the fact that both requirements need to be fulfilled for consent to be lawful. Another legal-technical but important aspect that most criticisms of consent do not address, concerns the distinction between the legal grounds of consent and contract. When criticizing consent, both EU and US authors often refer to a practice that is commonly known as “notice and consent” (agreeing in exchange for getting a service on the internet) but that does not necessarily constitute consent in the sense of EU data protection law, since it could also be regarded as “necessary for the performance of a contract” from a controller's perspective. Thus, what can be learned from the literature review is both too broad, omitting the legal complexities of consent, and too narrow, passing over the embeddedness of these critiques in wider professional and societal discourses. The remainder of this paper seeks to address these two points by analyzing the consent paradox in a more empirical fashion, zooming into the consent debate among German data protection practitioners.

3 Study and Methods: Analyzing the Consent Paradox through the Lens of German Data Protection Specialists

3.1 Case Selection: The German Consent Debate

To reconstruct the consent paradox in more detail, I conducted a discourse analysis of the consent debate among German data protection professionals between 2000 and early 2017. Before discussing how this analysis can help to address the broader issue of the consent paradox, it should be noted that the rationale for this kind of analysis comes from political sociology, which assumes that professionals shape important political questions in their respective areas of expertise [see 27]. Thus, I assume data

protection professionals and their debates influential for the development of consent and, consequently, worth analyzing.

Why is it worth looking at German data protection specialists in particular? First, the German tradition of data protection, informational self-determination, and consent has been influential in data protection at the European level [14, p. 54]. Second, it can be argued that the German discussion on consent was shaped by European and international debates, and therefore reflects the wider debate on consent to some extent. The most notable example of this mutual influence is the development of the EU legal framework for data protection as it has developed over time. Further, perhaps less obvious examples include transnational discussions on topics such as the “economics of privacy” [28], a theme that has made its way into the German debate in recent years. Third, the *form* of the German consent debate is distinct in that it has evolved as a hybrid of a scholarly, a societal, and a technical debate, involving academics, members of data protection authorities, and lawyers and data protection officers working in the private sector. However, I neither argue that the German debate has been decisive for the European field of data protection in general, nor do I claim that it merely reflects European or transnational developments. Rather, I want to demonstrate that the German debate, as a piece of the consent puzzle, can provide a useful starting point to understand the consent paradox. In particular, I expect these discussions to provide a more nuanced perspective on the technical details of consent in data protection law, which, as I have argued above, are notably absent from the scholarly debate on consent.

My analysis focuses on a period extending from the beginning of 2000 to March 2017. The research material consists of 27 written contributions to the consent debate, most of them taking the form of articles in professional journals (n=23), some contributions to edited volumes (n=3), and one research report. Due to the time-consuming interpretative method used (see below), it was not possible to include entire monographs.

The process of selecting these texts involved multiple stages. I first identified a series of influential, that is, frequently cited, articles on consent in data protection journals by compiling references from the authoritative legal commentary on the Germany Federal Data Protection Act (BDSG) [29, p. 432]. In addition, I compiled all of the references from the literature review chapters of recent dissertations on consent, assuming that they include the most important and recent work on the topic [30, 31]. In a second step, I systematically searched a major German database⁹ as well as Google scholar for German-speaking articles on consent in data protection. This was necessary to avoid reproducing potential citation bias from the first round of selection.¹⁰ After sorting out those articles that dealt primarily with consent in the medical field, I arrived at 92 texts, two-thirds of them from the period between 2000 and 2017.¹¹ The increasing number of articles on consent reflects a growing interest in the issue among

⁹ Database of the Berlin State Library: <http://staatsbibliothek-berlin.de/en/>.

¹⁰ A likely citation bias in this case could consist of authors who do not cite each other because they belong to different schools of thought.

¹¹ The exact numbers of texts for the respective decades are: 1970s (n=9), 1980s (n=9), 1990s (n=13), 2000s (n=27), 2010s (n=34).

data protection specialists since the turn of the millennium. This can be read as evidence of the consent paradox. Most of the articles published since 2000 discuss the importance of consent in the dawning age of commercial Internet usage and the associated business model of offering services in exchange for monetizing user data. As this discussion seems to be at the core of the consent debate, I decided to focus on these articles and exclude texts written before 2000¹². I further excluded the few texts since 2000 that dealt with consent in the offline world, for instance, in the case of loyalty programs [see 14, p. 195]. This left a total of 37 articles for the document analysis. This number was further reduced to 27 in the process of interpretation, which I turn to in the following.

3.2 Method: Making Sense of the Consent Debate with the Help of Discourse Analysis and Grounded Theory

To analyze the material selected, I conducted a *discourse analysis*. Discourse analysis does not rely on a prescribed theory or method, but rather denotes a methodological standpoint. Discourse analysis encompasses different schools of thought, sharing the premise that reality is shaped by *discourse*. Discourse can be defined as “ideas, concepts, and categories through which meaning is given to social and physical phenomena” [32]. In short, discourses are knowledge orders, underlying arguments and debates. At the same time, discourses often come with certain narratives, which, as Gottweis put it, have the “power to create order” [33, p. 468]. Thus, in discourse analysis, knowing and telling blend into each other. Even the most technical debates rely on certain views and assumptions to make sense of what they are doing. Most discourse analyses aim at identifying discourses in spoken and written language. The role of discourse in data protection has not been studied sufficiently in the research to date. A notable exception¹³ is Bennett and Raab’s argument that the field of data protection and privacy has been shaped by a discourse they call the “privacy paradigm,” which links actors’ “agreed understanding of the nature and the scope” of privacy to the values of liberal democracy and the autonomous individual [34, p. 13]. Bennett and Raab have shown that these assumptions are not merely rhetoric but have substantial and wide-ranging implications, including the focus on *personal data* in data protection law [34, p. 16].

Applying discourse analysis to a complex legal issue such as data protection involves going beyond the analysis of law itself. As Klein et al. argue in the area of copyright law, legal arguments rely on non-legal justifications that in turn are connected to broader narratives, making them appear as compelling arguments [35]. It is important to note that competing justifications or discourses are often rooted in fundamentally different understandings of what is “good, right, and just” [35, p. 4]. This also implies that there can be no single understanding of, in our case, data protection

¹² I allowed for a tolerance of one year, assuming that a text published in 1999 was written around the turn of the millennium.

¹³ Bennett and Raab’s work is not the only exception. I refer to other recent works on data protection’s discourses in the conclusion.

or their respective aims. Rather, there are different and conflicting ways of thinking about data protection and the role of consent therein. As Bennett and Raab have shown, these different ways of meaning making, in turn, lead to different (interpretations of) the legal framework and regulatory options. Discourse analysis goes further than a literature review that merely summarizes the arguments made: It aims at explicitly identifying the worldviews and assumptions underpinning those arguments. I consider those underpinnings an important part of the consent paradox, since they can help to explain why certain views of consent persist while others are rejected or, at least, less prominent.

Since discourse analysis does not prescribe a specific method to identify *discourses* in the research material, I employed *grounded theory*, a framework for qualitative data analysis. Grounded theory aims at deriving a “theory” from a recursive interpretation of data [36, p.12]. In this context, “theory” means abstracting underlying concepts “that can be used to explain or predict phenomena” [36, 15]. As others have shown, grounded theory ties in well with discourse analysis since both share the aim of discovering explanations that are not manifest in the data [see 37, p. 237]. In the case of texts, this means that reading and summarizing them is not enough: they need to be interpreted instead. Grounded theory provides the tools for such an interpretation. It allows for “reading between the lines” in a controlled manner.¹⁴ Thus, I consider grounded theory a helpful tool to identify the discourses shaping the consent paradox.

Grounded theory is based on a multi-staged interpretation process. It begins with “breaking down” the data “into discrete parts”, that is, single words and sentences [36, p. 102]. These parts are examined, shedding light on specific terms and connections that remain invisible in the usual approach of reading and summarizing. From these newly discovered meanings, hypotheses for interpretation are developed and tested against the material. This recursive process is supported by techniques such as asking generative questions (who, what, why, how), making comparisons in the data, and placing the data into categories and sub-categories. The aim of grounded theory is to “open up the text” [36, p. 102] in order to develop ideas about underlying concepts, refine them in the light of the material, and test them against old and newly added material. The goal of this exercise is to “reassemble” the material in a new and illuminating way [36, p. 102]. New texts are added until a point of saturation has been reached, which means that nothing new is brought to the fore by adding more material [36, p. 214]. In my case, I reached this point after interpreting 27 texts. To organize the interpretation process, I used the qualitative data analysis software MAXQDA, which makes it possible to visualize and perform the procedure of assigning attributes to text segments, referred to as “coding” in qualitative and interpretative research [39, p. 3]. As findings from interpretative research and discourse analysis take the form of narratives and rationales, they cannot be presented as graphs and numbers. They are usually presented first as a comprehensive, evidence-rich analysis, allowing the reader to clearly understand the interpretation derived from the material [see 40, p. 113].

¹⁴ However, interpretative studies do not and cannot aspire to the same goals and evaluative standards as positivist research [see 38].

As I will discuss in the following, I was able to reconstruct two different discourses on consent from the material: the *world of data protection rules* and the *data market world*¹⁵. These two discourses correspond to the two major critiques of consent: *freely given* and *informed consent*. Furthermore, I argue that my findings complement the literature review in section 2. First, they provide a more nuanced understanding of the technical details of the consent debate and the relationship between freely given and informed consent. Second, and at the same time, they provide a broader picture by linking the technical arguments to broader societal discourses, thus explaining their influence (or their lack thereof).

4 The Two Worlds of Consent in Data Protection

In the following I discuss the two predominant discourses of consent that I have identified among German data protection professionals: the *world of data protection rules* and the *data market world*.¹⁶ I use these terms as a kind of shorthand to distinguish the two most common ways of discussing consent in data protection among German data protection specialists. I introduce both worlds in their own words—to the extent possible in an English-speaking publication drawing on German texts. Presenting both worlds in their own language allows the reader to grasp each one’s own reality [see 41, p. 153]. For example, whereas the *data market* appears as profit-driven to the critical observer, it produces mutual benefits from its own perspective.¹⁷ I argue that each world’s stance on consent depends on these kinds of narratives, which makes it important to present each in its own right.

I distinguish both worlds based on their different (1) understanding of data protection’s aims and rationales, (2) their view on the relationships between and responsibilities of data controllers and data subjects, and (3) their approach to consent in the Internet age. In accordance with my methodology, these categories emerged from the interpretation process. Consequently, the material also revealed which text and which author belongs to which camp. Discourse theory, however, assumes that discourses reach beyond their authors, embodying broader worldviews that authors make use of and modify but do not create on their own [see 42, p. 11]. Thus, while referring to specific texts, I foreground the competing ideas and worldviews on consent and data protection instead of their authors. These discursive patterns, I argue, can provide insights beyond the specificities of the German case. The main tenets of each world are summarized in table 1.

¹⁵ The term “world” is widely used in constructivist social science to foreground the fact that discourses produce different “realities” [see 41, p. 125]. In the following, I use the term interchangeably with discourse.

¹⁶ In my master’s thesis, I made a more fine-grained distinction of discourses on consent, resulting in four different worlds. For this paper, I reduced complexity by leaving out one discourse and merging two others. This also explains why, in the following, I do not cite all 27 texts analyzed.

¹⁷ I thank one of the anonymous reviewers for the question that led to this clarification.

4.1 The World of Data Protection Rules

The first discourse I identified in the German consent debate is the *world of data protection rules*. The world of data protection rules emphasizes *informational self-determination* as its higher aim [43, see 44, 45], but in a relatively formalistic manner that does not explain well the rationale behind this camp's stance on data protection and consent. The world of data protection rules' way of thinking and arguing can be characterized more accurately as a bureaucratic or regulatory one.¹⁸ It is concerned with the rigorous application of a hierarchical set of rules, instruments, and criteria. It values rules that are "explicit"¹⁹, "comprehensive", and "precise" [see 44, 46, 47]. Adhering to the logic of *functionality*, data protection rules are both means and ends. Consent is "good right and just" when it fulfills the criteria laid out in data protection rules. This is a challenging task because, as one author has noted, "a number of substantial, formal and other requirements must be met" [47, p. 727]. These requirements are set out in general and specific data protection laws²⁰ and elaborated further through the decisions of courts and data protection authorities and in legal commentary. In sum, the world of data protection rules understands data protection as a complex set of regulations—a machinery that needs to be put to work.²¹

In the world of data protection rules, it is the data controller who bears the burden of compliance [see 46]. Consequently, the world of data protection rules refers to the data controller as the *verantwortliche Stelle*, which literally translates as "responsible authority" [see 45, p. 725]. The data subject, in turn, is addressed as "affected person" (*Betroffener*). The assumption behind these terms is that controllers' data processing practices can have negative effects on data subjects. More generally, the world of data protection rules assumes a certain imbalance between data subjects and controllers [43, p. 404, 46, p. 91]. Meaningful consent needs to reflect this imbalance.

The asymmetry between data subjects and controllers is addressed through the requirement that any consent must be freely given. While, in fact, all requirements for valid consent must be met, it is the issue of freely given consent that dominates the world of data protection rules' discussions. The world of data protection rules holds that consent cannot be freely given in situations where the data subject is confronted with the "coercive power of the state", "irresistible incentives", or "legal and factual dependencies" [46, p. 92]. In those instances, the data subject's decisional autonomy is limited.

German data protection law's concept of "linkage prohibition" (*Koppelungsverbot*) specifies the requirement of freely given consent in certain situations of factual dependencies. It forbids that data controllers "depend the conclusion of a contract on the consent of the data subject for advertising or for marketing/opinion research purposes, when the data subject does not have alternative access to comparable contractual ser-

¹⁸ I thank Kjetil Rommetveit who suggested these terms to me.

¹⁹ All direct quotations from German sources are my translations.

²⁰ The laws those texts mainly refer to are the German Federal Data Protection Act (BDSG) and the German Telemedia Act (TMG).

²¹ This characterization is inspired by Boltanski and Thévenot's description of an industrial way of thinking and acting [41, p. 203].

vices without the consent or such an alternative is not possible in a reasonable way” [translation by Kosta, see 14, p. 194]. In other words, denying consent for marketing purposes will not lead to a denial of access to a particular service [see 45, p. 709]. From this viewpoint, freely given consent differs from a contract, in which one party imposes certain conditions upon the other. The linkage prohibition thus offers a litmus test for assessing whether consent has been freely given. It relies upon the purpose limitation principle as well as an assessment of the data controller’s market position.²² The linkage prohibition and its underlying principles are key in understanding the world of data protection rules’ critique of consent in the Internet age.

The world of data protection rules holds that the practice of “paying with data” for online services is difficult to reconcile with the requirement of freely given consent. Its advocates arrive at this conclusion based on the ideas expressed in the linkage prohibition. First, they argue that consent in the context of information society services (*Telemediendienste*) need to be assessed by asking whether their users can access the service without consenting to the usage of data for advertising purposes. A second and related, question is whether there are alternatives that fulfill this criterion [43, p. 405, see 44, p. 648]. Since major online services or platforms do not offer this possibility or can be considered monopolies [see 48, p. 113], the linkage prohibition is often violated. Thus, there are very few situations where consent can be deemed freely given: only those in which consent and contract have been unbundled from each other [49, p. 82]. In the majority of situations, data processing must be based on other grounds than consent, such as contracts, sector-specific laws, or codes of conduct and certification schemes as a more flexible alternative [see 49, p. 82]. Consequently, it is only in those rare situations where consent can be considered freely given that the issue of informed consent eventually becomes relevant [see 43, p. 408, 50, p. 145].

To summarize, the world of data protection rules calls into question *whether* data protection in the Internet age can continue to rely on consent. However, its operationalization of the imbalance between individuals and data controllers presents a kind of quiet critique of power, embodying bureaucratic rather than fundamental rights-related values. Put differently, consent appears problematic for the modest reason that it does not tick the box on freely given consent. The world of data protection rules appears rather self-referential, lacking a compelling narrative of why power asymmetries endanger freely given consent.

4.2 The Data Market World

The second discourse among German data protectionists is the *data market world*. From the data market viewpoint, data protection serves the higher goal of creating *mutual benefits* by facilitating the exchange of personal data between data subjects and controllers. Its advocates claim that data markets present a win-win-situation,

²² Interestingly, the new GDPR introduces a linkage prohibition in its Article 7(4). In contrast to the older German linkage prohibition, the provision in the GDPR is not limited to situations of using personal data for marketing purposes.

asserting that it is not just companies but also their customers who benefit from data driven business models [see 51 p. 18]. The fact that data subjects do benefit from the data market becomes visible when observing users' behavior: Users do not refrain from using services, but deliberately give their data to benefit from data processing. The data market provides them with a number of useful and indispensable services such as social networks [see 52, p. 635]. The principle of "paying with data" has become an accepted part of users' lived reality [see 53, p. 499].

The data market's thesis is that data protection should be more *evidence-based*. Its advocates call for an empirically informed understanding of modern data processing and user behavior. While earlier works mention those new realities in a rather anecdotal manner [see 51, 54], more recent contributions build their arguments on actual scientific evidence, referring to works on the "economics of privacy" [see 55, 56]. These insights, whether anecdotal or empirical, need to be reflected in data protection law and, in turn, in its operationalization of consent. Articulating this fact-based rationale, the data market world distinguishes itself from the world of data protection rules. Some of its earlier contributions, in particular those from before 2010, refer directly to the contributions from the world of data protection rules [see 54, 57]. As one data market advocate puts it, the other side, that is, the world of data protection rules, "understands self-determination as an end in itself" [54, p. 1622]. They criticize that the world of data protection rules' understanding of data protection is detached from actual harms and in ignorance of individuals' deliberate choices to decide for themselves on the risks and benefits of data processing.

The data market world understands data subjects as "customers" [see 53, 54]. More recent works refer to data subjects as "users" [see 55, 56]. The notions of "customer" and "user" suggest a more active role for the data subject—compared to the "affected person" in the world of data protection rules. Further, the terms imply that data subjects have commercial interests reaching beyond the mere expectation of having their data protected. In more technical terms, the data market world argues that the right to informational self-determination includes the idea of granting data subjects a commercial interest and, going even further, a certain leverage in commercializing their personal data [see 52, p. 639]. The German general right to personality has been increasingly interpreted in favor of a commercialization of the personality [see 57, p. 43]. Since the right to informational self-determination is also based on the right to personality, it is "only a small step" [52, p. 639] from understanding the commercial exchange of personal data as an expression of informational self-determination. Against this backdrop, consent is considered not only a suitable, but also a central instrument for enabling transactions of personal data [see 57, p. 43]. What sets the data market world's understanding of consent apart from the world of data protection rules is that the concepts of consent and contract do not differ but converge [52, p. 640].

In contrast to what its critics might assume, the data market world does not deny a certain imbalance between both parties [see 52, p. 639]. Yet, it would be a mistake to jump to "paternalistic" conclusions [see 52, p. 637]. Data protection should not protect users against themselves [53, p. 499]. The imbalance between data subjects and controllers is not ultimately harmful. Quite the contrary, most commercial data pro-

cessing is harmless and, in fact, often beneficial to the data subject [see already 51, p. 18]. However, to be able to weigh the risks and benefits, the user needs to be informed about the modalities of the transaction. Most importantly, it must be made clear to the user that the service is not free to her but that she is, in fact, paying with her data [see 57, p. 41, 58, p. 159]. In short, the data market world highlights the problem of information asymmetries and the requirement of redressing them through the requirement of informed consent.

Yet, the data market world does not entirely dispense with the requirement of freely given consent and the related concept of linkage prohibition. In my analysis, I observed two ways how its proponents deal with the issue of freely given consent. The first one is to reinterpret what “freely given” means. Some authors propose to reserve the notion of freely given consent, and thus the linkage prohibition, for those situations where the data controller is a public authority, an employer [58, p. 158] or where there is a “coercive” dependency, as in the case of banking or insurance contracts [53, p. 504]. Information society services, in contrast, should not by default be subject to the linkage prohibition [see already 59, p. 399]. In most cases, freely given consent can be incorporated into the requirement for informed consent instead: “A person who is not informed cannot assess the implications of its decision and thus is not giving consent freely.” [60, p. 156]. Yet, this positioning remains largely unexplained. The implicit assumption seems to be that a strict application of the linkage prohibition is “removed from reality”, since the linkage prohibition forbids what is considered the “life blood” [52, p. 637] of the relationship between users and Internet platforms: the further processing of personal data in exchange for using a service. The second way in which the world of the data market deals with the issue of freely given consent is by omitting it, focusing on the informedness of consent instead. This development is evidenced by the introduction of the term “informed consent” into the German debate [see 55, 56, 61]. Along with it comes a burgeoning literature on how to improve informed consent, ensuring that data subjects read and understand privacy policies and decide in their best interest [see 24]. The concrete measures that are discussed concern the idea to simplify privacy policies into “one pagers” and privacy icons [55]. Another related discussion concerns the idea of improving young peoples’ data protection literacy [62, p. 769]. Finally, technical means to support users’ informed consent are discussed in this context [see already 51, p. 19].²³ While those two options of sidestepping the issue of freely given consent appear rather separate from each other, they have at least two things in common. First, they embody an evidence-based approach to data protection, drawing on insights into users’ everyday reality. Second, although appearing grounded in facts rather than norms, both options reify the normative value of user choice and thus consent.

In sum, for the data market world, the question is not whether but *how* consent can be implemented within data protection. Presenting itself as a fact-based and pragmatic way of reasoning, the data market world does not give the impression of being ideologically charged. Its aims and rationale lead the data market world to a reformist problematization of consent. Speaking of reforms, the data market world is quite spe-

²³ The latter examples are not confined to the discussion on ensuring informed consent.

cific when it comes to improving the informedness of consent. However, its advocates remain rather vague on other important questions, such as what the concrete implications of a more contractual understanding of consent are.

Table 1. Discourses on consent among German data protectionists between 2000 and 2017.

	World of data protection rules	Data market world
Higher aim of data protection	Right to informational self-determination	Beneficial data economy
Logic of argumentation	Bureaucratic (compliance)	Evidence-based (correspondence with reality)
Relations between data subjects and data controllers	Power asymmetry	Information asymmetry
Operationalization of consent	Freely given consent Consent \neq contract Linkage prohibition	Informed consent Consent \sim contract Ensuring informed choice
Future of consent	Uncertain (<i>whether</i>)	Reformist (<i>how</i>)
Emblematic texts	[43–49]	[51–56, 58, 58, 59]

5 Discussion and Conclusion: Data protection as a Critique of Power

In this paper, I have set out to account for the *consent paradox*, that is, the prominent role ascribed to consent in data protection despite its numerous critiques. To elucidate the consent paradox, I first reviewed the scholarly critiques of consent. I showed that critiquing consent in terms of information asymmetries confirms rather than calls into question the prominent role of consent and thus reproduces the consent paradox. A problematization of consent based on power asymmetries, in contrast, provides a more substantive critique of consent, casting doubts on the centrality of consent in data protection. Yet, the literature review appeared too broad and too narrow at the same time. On the one hand, it did not tell us much about the legal technical consequences of the respective arguments. On the other hand, the literature review could not account for the fact that criticizing consent in terms of information asymmetries is more common than problematizing consent in the language of power asymmetries. To address these gaps, I supplemented the literature review by conducting a discourse analysis of the debate on consent among German data protection professionals, distinguishing two common ways of discussing consent. Problematizing consent in terms of power asymmetries is linked to the discourse of data protection rules, which stresses data subjects' dependence on digital platforms, and for that reason, calls into question *whether* data protection can continue to rely on consent. It, however, fails to provide a coherent narrative articulating why power asymmetries are problematic. The fact that consent, when given in situations of factual dependency, might result in non-compliance with data protection law, does not present a particularly powerful narra-

tive. Highlighting information asymmetries, in contrast, is linked to the popular and intuitive narrative of the data market. The data market discourse is supported by an evidence-based approach of reasoning. On the data market, consumers exchange “their data” in order to benefit from the services provided by internet companies. As a last word of caution, the worlds of *data protection rules* and the *data market* represent ideal types: They are scientific constructs to make sense of a more complex reality. They neither explain all aspects of the consent debate, nor necessarily correspond to the intentions of the actors therein. For example, conducting a research project that improves the informedness of consent does not necessitate the researcher to be convinced or even aware of the data market discourse.²⁴

Among scholars it is conventional wisdom that the meaning of data protection is far from settled [see 19, p. 272] and maybe even “impossible to define” [see 63, p. 330]. Yet, the search for data protection’s meaning goes beyond the realm of data protection law. It is also influenced by wider societal discourses and conflicts. My discussion of the consent paradox speaks to an emerging strand of literature exploring how political, scientific and popular discourses shape the field of data protection [21, 64–67]. Quite a few of those works come to similar conclusions: They observe an increasing individualization and commodification of data protection [10, 21, 64, 65]. It is tempting to dismiss these studies as broad and undifferentiated attempts to explain developments in data protection as influenced by a neoliberal zeitgeist. In fact, these studies paint a more nuanced picture, attempting to show (1) how data protection oscillates between different aims and understandings, most notably the free flow of data and the protection of individuals [see 63, p. 336], (2) how these understandings translate into laws and instruments and vice versa [see 64], and (3) how the field and its perceptions change over time [see 7]. Yet, further research is needed on all three points.

Looking at the case of the consent paradox, future work needs to retrace in more detail how the world of data protection rules, the data market world, or varieties of those discourses shape the interpretation of freely given and informed consent in practice, especially under the new GDPR. The EU’s new data protection rules leave room for interpretation on these points, especially in their take on the linkage prohibition in article 7(4) and recital 43. In this analysis, I have suggested that freely given consent could be incorporated into the requirement of informedness, thus redefining power asymmetries as information asymmetries. Another possibility that is more in line with the world of data protection rules is a strong take on the linkage prohibition. This, in turn, could reduce the omnipresence of consent in practice, leading data controllers to rely on other legal grounds, most importantly contracts. However, this might only shift the discussion over take-it-or-leave-it choices from the legal ground of consent to that of contracts [see 22, p. 7].²⁵ Another research gap left by my study concerns the development of the consent debate and its underlying discourses over time. Due to

²⁴ Matzner et al. make the same point in the context of the German “DIY data protection discourse” [21, p. 289].

²⁵ During the finalization phase of this article, the discussion on how to deal with the linkage prohibition and take-it-or-leave-it choices in the GDPR has just begun [68, 69].

its research design, my paper does not account for this diachronic perspective in a representative manner. It only allows for the tentative hypothesis that the data market discourse has become more dominant in recent years.

What are the practical consequences of my findings? Asking this question implies that I consider the “consent paradox” not only an empirical phenomenon but also as a political problem. The consent paradox is problematic since it discourages more comprehensive critiques on the limits of consent and thus hinders more substantial reforms to consent. As others have proposed, meaningful reforms of consent should include reducing the burden on consent by regulating what kind of processing practices can be subject to individual choice in the first place [see 70, p. 527]. The omnipresence of consent also limits our ability to think beyond consent, tying up resources needed to advance in other issue areas of data protection such as organizational and enforcement measures [see 5]. Finally, the consent paradox and its underlying market discourse risks omitting the collective values of data protection and privacy [see 65, p. 94]. My analysis suggests that a break with the consent paradox can only be achieved by reintroducing a more compelling critique of power into data protection than the rule-oriented and bureaucratic data protection discourse is able to articulate. As others have argued, the early justifications of data protection with their focus on holding the powerful accountable might be instructive for this purpose [7, 71]. Articulating data protection as a critique of power necessitates us to make clear how power and data processing relate to each other, what are the risks associated with it, and consequently, what should be the ends and means of data protection.

References

1. Bergemann, B.: Der „informed consent“ im Datenschutz: Eine politikwissenschaftliche Analyse, Master thesis. Freie Universität Berlin. <https://www.econstor.eu/handle/10419/162861>, (2017).
2. Schermer, B.W., Custers, B., van der Hof, S.: The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. *Ethics Inf. Technol.* (2014).
3. Boltanski, L., Chiapello, È.: *The new spirit of capitalism*. Verso, London (2007).
4. Austin, L.M.: Enough About Me: Why Privacy is About Power, not Consent (or Harm). In: Sarat, A. (ed.) *A World without Privacy: What Law Can and Should Do?* pp. 131–189. Cambridge University Press, New York, NY (2014).
5. Zanfir, G.: Forgetting About Consent. Why The Focus Should Be On “Suitable Safeguards” in Data Protection Law. In: Gutwirth, S., Leenes, R., and De Hert, P. (eds.) *Re-loading Data Protection*. pp. 237–257. Springer Netherlands, Dordrecht (2014).
6. Koops, B.-J.: The trouble with European data protection law. *Int. Data Priv. Law.* 4, 250–261 (2014).
7. van der Sloot, B.: Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. *Int. Data Priv. Law.* 4, 307–325 (2014).
8. Barocas, S., Nissenbaum, H.: Big Data’s End Run around Anonymity and Consent. In: Lane, J., Stodden, V., Bender, S., and Nissenbaum, H. (eds.) *Privacy, Big Data, and the*

- Public Good: Frameworks for Engagement. pp. 44–75. Cambridge University Press, Cambridge (2014).
9. Rouvroy, A., Poulet, Y.: The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In: Gutwirth, S., Poulet, Y., De Hert, P., de Terwangne, C., and Nouwt, S. (eds.) *Reinventing Data Protection?* pp. 45–76. Springer Netherlands, Dordrecht (2009).
 10. Crain, M.: The limits of transparency: Data brokers and commodification. *New Media Soc.* (2016).
 11. McDermott, Y.: Conceptualising the right to data protection in an era of Big Data. *Big Data Soc.* 4, (2017).
 12. Manson, N.C., O’Neill, O.: *Rethinking informed consent in bioethics.* Cambridge University Press, Cambridge (2007).
 13. Laurie, G.T.: *Genetic privacy: a challenge to medico-legal norms.* Cambridge University Press, Cambridge (2004).
 14. Kosta, E.: *Consent in European data protection law.* Martinus Nijhoff Publishers, Leiden (2013).
 15. Bennett, C.J.: *The privacy advocates: resisting the spread of surveillance.* MIT Press, Cambridge, MA (2008).
 16. Gutwirth, S.: Short statement about the role of consent in the European data protection directive. *Vrije Universiteit Brussel, Brussels* (2012).
 17. De Hert, P., Papakonstantinou, V.: The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Comput. Law Secur. Rev.* 32, 179–194 (2016).
 18. Quelle, C.: Not just User Control in the General Data Protection Regulation. In: Lehmann, A., Whitehouse, D., Fischer-Hübner, S., Fritsch, L., and Raab, C. (eds.) *Privacy and Identity Management. Facing up to Next Steps.* pp. 140–163. Springer International Publishing, Cham (2016).
 19. Lysnsky, O.: *The foundations of EU data protection law.* Oxford University Press, Oxford (2015).
 20. von Uckermann, E.F.: Einwilligung nach BDSG – ein Mißverständnis? *Datenschutz Datensich. DuD.* 3, 163–168 (1979).
 21. Matzner, T., Masur, P.K., Ochs, C., von Pape, T.: Do-It-Yourself Data Protection—Empowerment or Burden? In: Gutwirth, S., Leenes, R., and De Hert, P. (eds.) *Data Protection on the Move.* pp. 277–305. Springer Netherlands, Dordrecht (2016).
 22. Rhoen, M.: Beyond consent: improving data protection through consumer protection law. *Internet Policy Rev.* 5, (2016).
 23. Solove, D.J.: Privacy Self-Management and the Consent Dilemma. *Harv. Law Rev.* 126, 1880–1903 (2013).
 24. Arnold, R., Hillebrand, A., Waldburger, M.: *Personal Data and Privacy. Final Report (Study for Ofcom).* WIK-Consult, Bad Honnef (2015).
 25. Acquisti, A., Sleeper, M., Wang, Y., Wilson, S., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F.: Nudges for Privacy and Security: Understanding and Assisting Users’ Choices Online. *ACM Comput. Surv.* 50, 1–41 (2017).

26. Calo, R.: Against Notice Skepticism In Privacy (And Elsewhere). *Notre Dame Law Rev.* 87, 1027–1072 (2012).
27. Kauppi, N., Madsen, M.R. eds: *Transnational power elites: the social and global structuration of the EU*. Routledge, London (2013).
28. Acquisti, A., Taylor, C.R., Wagman, L.: *The Economics of Privacy*. Social Science Research Network, Rochester, NY (2016).
29. Simitis, S. ed: § 4a Einwilligung. In: *Kommentar zum Bundesdatenschutzgesetz*. pp. 432–466. Nomos, Baden-Baden (2011).
30. Rogosch, P.M.: *Die Einwilligung im Datenschutzrecht*. Nomos, Baden-Baden (2013).
31. Hermstrüwer, Y.: *Informationelle Selbstgefährdung: zur rechtsfunktionalen, spieltheoretischen und empirischen Rationalität der datenschutzrechtlichen Einwilligung und des Rechts auf informationelle Selbstbestimmung*. Mohr Siebeck, Tübingen (2016).
32. Hajer, M.: FAQ, http://www.maartenhajer.nl/?page_id=14.
33. Gottweis, H.: *Argumentative Policy Analysis*. In: Peters, G. and Pierre, J. (eds.) *Handbook of Public Policy*. pp. 461–479. Sage, London (2006).
34. Bennett, C.J., Raab, C.D.: *The governance of privacy: policy instruments in global perspective*. Ashgate, Aldershot (2003).
35. Klein, B., Moss, G., Edwards, L.: *Understanding copyright: intellectual property in the digital age*. SAGE, Los Angeles, CA (2015).
36. Strauss, A.L., Corbin, J.M.: *Basics of qualitative research: techniques and procedures for developing grounded theory*. Sage Publications, Thousand Oaks, CA (1998).
37. Keller, R.: *Analysing Discourse. An Approach From the Sociology of Knowledge*. *Forum Qual. Sozialforschung Forum Qual. Soc. Res.* 6, (2005).
38. Haverland, M., Yanow, D.: A Hitchhiker’s Guide to the Public Administration Research Universe: Surviving Conversations on Methodologies and Methods. *Public Adm. Rev.* 72, 401–408 (2012).
39. Saldaña, J.: *The coding manual for qualitative researchers*. SAGE, Los Angeles, CA (2009).
40. Schwartz-Shea, P., Yanow, D.: *Interpretive research design: concepts and processes*. Routledge, New York, NY (2012).
41. Boltanski, L., Thévenot, L.: *On justification: economies of worth*. Princeton University Press, Princeton (2006).
42. Fischer, F., Gottweis, H.: Introduction: The Argumentative Turn Revisited. In: Fischer, F. and Gottweis, H. (eds.) *The argumentative turn revisited: public policy as communicative practice*. pp. 1–27. Duke University Press, Durham (2012).
43. Menzel, H.-J.: *Datenschutzrechtliche Einwilligungen: Plädoyer für eine Rückkehr zur Selbstbestimmung*. *Datenschutz Datensicherheit DuD.* 32, 400–408 (2008).
44. Schaar, P.: *Datenschutzrechtliche Einwilligung im Internet*. *Multimed. Recht MMR.* 2001, 644–648 (2001).
45. Iraschko-Luscher, S.: *Einwilligung – ein stumpfes Schwert des Datenschutzes?* *Datenschutz Datensicherheit DuD.* 30, 706–710 (2006).
46. Roßnagel, A., Pfitzmann, A., Garstka, H.: *Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern*. Bundesministerium des Innern, Berlin (2001).

47. Zscherpe, K.: Anforderungen an die datenschutzrechtliche Einwilligung im Internet. *Multimed. Recht MMR*. 2004, 723–727 (2004).
48. Kutscha, M.: Mehr Datenschutz — aber wie? *Z. Für Rechtspolit. ZRP*. 43, 112–114 (2010).
49. Kamp, M., Rost, M.: Kritik an der Einwilligung. Ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen. *Datenschutz Datensicherheit DuD*. 37, 80–84 (2013).
50. Körner, M.: Informierte Einwilligung als Schutzkonzept. In: Simon, D. and Weiss, M. (eds.) *Zur Autonomie des Individuums: Liber Amicorum für Spiros Simitis*. pp. 131–150. Nomos, Baden-Baden (2000).
51. Ladeur, K.-H.: Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken. Zur “objektiv-rechtlichen Dimension” des Datenschutzes. *Datenschutz Datensicherheit DuD*. 24, 12–19 (2000).
52. Bräutigam, P.: Das Nutzungsverhältnis bei sozialen Netzwerken - Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten. *Multimed. Recht MMR*. 2012, 635–641 (2012).
53. Schafft, T., Ruoff, A.: Nutzung personenbezogener Daten für Werbezwecke zwischen Einwilligung und Vertragserfüllung. *Comput. Recht CR*. 22, 499–504 (2006).
54. Bull, H.P.: Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese? *Neue Juristische Wochenschr. NJW*. 59, 1617–1623 (2006).
55. Pollmann, M., Kipker, D.-K.: Informierte Einwilligung in der Online-Welt. *Datenschutz Datensicherheit DuD*. 40, 378–381 (2016).
56. Arnold, R., Hillebrand, A., Waldburger, M.: Informed Consent in Theorie und Praxis: Warum Lesen, Verstehen und Handeln auseinanderfallen. *Datenschutz Datensicherheit DuD*. 39, 730–734 (2015).
57. Buchner, B.: Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument. *Datenschutz Datensicherheit DuD*. 34, 39–43 (2010).
58. Buchner, B.: Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO. *Datenschutz Datensicherheit DuD*. 155–161 (2016).
59. von Lewinski, K.: Privacy Policies: Unterrichtungen und Einwilligung im Internet. *Datenschutz Datensicherheit DuD*. 26, 395–400 (2002).
60. Petri, T.: Datenschutzrechtliche Einwilligung im Massengeschäftsverkehr. *Recht Datenverarb. RdV*. 23, 153–158 (2007).
61. Beisenherz, G., Tinnefeld, M.-T.: Aspekte der Einwilligung: Zivil- und strafrechtliche Bezüge der Einwilligung im Datenschutzrecht. *Datenschutz Datensicherheit DuD*. 35, 110–115 (2011).
62. Caspar, J.: Soziale Netzwerke – Endstation informationelle Selbstbestimmung?: Ein Bericht aus der Behördenpraxis. *Datenschutz Datensicherheit DuD*. 37, 767–771 (2013).
63. Bellanova, R.: Digital, politics, and algorithms: Governing digital data through the lens of data protection. *Eur. J. Soc. Theory*. 20, 329–347 (2017).
64. Draper, N.A.: From Privacy Pragmatist to Privacy Resigned: Challenging Narratives of Rational Choice in Digital Privacy Debates: Challenging Rational Choice in Digital Privacy Debates. *Policy Internet*. 9, 232–251 (2017).
65. Hull, G.: Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics Inf. Technol.* 17, 89–101 (2015).

66. Bellanova, R.: Data Protection, with Love. *Int. Polit. Sociol.* 8, 112–115 (2014).
67. van Dijk, N., Gellert, R., Rommetveit, K.: A risk to a right? Beyond data protection risk assessments. *Comput. Law Secur. Rev.* 32, 286–306 (2016).
68. Borgesius, F.J.Z., Kruikemeier, S., Boerman, S.C., Helberger, N.: Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. *Eur. Data Prot. Law Rev.* 3, 353–368 (2017).
69. Article 29 Data Protection Working Party: Guidelines on Consent under Regulation 2016/679. WP 259 (2017).
70. Gellert, R., Gutwirth, S.: The legal construction of privacy and data protection. *Comput. Law Secur. Rev.* 29, 522–530 (2013).
71. Rauhofer, J.: One Step Forward, Two Steps Back? Critical observations on the proposed reform of the EU data protection framework. University of Edinburgh School of Law, Edinburgh (2013).