The role of the trust category for the development of new data protection approaches

Markus Uhlmann, Universität Kassel, Germany

Kris Shrishak, Technische Universität Darmstadt, Germany

Michael Weiler, Goethe Universität Frankfurt, Germany

1. Introduction

That regulatory approaches and normative principles of data protection are challenged in a myriad of ways is a widespread belief that is shared among data protection advocates and scientists of various disciplines (e.g., Hagendorff 2017; Koops 2014; Roßnagel 2016). Almost all comments on current data protection regulation agree that especially data intensive socio-technical developments like the emergence of online social network sites (OSNs) such as Facebook or big data are the main driving forces that challenge data protection (Türpe et al. 2017). For example, data protection regulation on the basis of notice-and-choice and data protection principles like data minimization, purpose binding or transparency is deeply challenged through big data (Mayer-Schönberger/ Padova 2016). Especially the reliance on the idea of informational self-determination in terms of individual information control seems no longer appropriate when users are confronted with powerful organizations that collect vast amounts of data (Hartzog 2018). However, not only technological developments challenge existing data protection regulation, some authors also emphasize the fact that the normative rationality of contemporary networked privacy practices that are established among users of OSNs are desynchronized from normative principles of data protection. While users constitute data intensive privacy practices, data protection tries to enforce normative principles like data limitation and individual information control that contradict user practices (Marwick/ boyd 2014; Ladeur 2015; Ochs/ Büttner 2018; Stalder 2011). Another critique refers to the fact that data protection is not able to capture the right issues that are currently at stake. In this context, existing normative concepts of data protection such as personal identifiable information that are primarily concerned with the protection of individual integrity cannot be applied to big data risks, which are related to the discrimination of networks and groups (Amoore 2014; Matzner 2014; Mantelero 2016; Oostveen 2016). Therefore, some critiques of current data protection argue that protecting the integrity of networks and groups become the condition for protecting individual privacy (Floridi 2017). Furthermore, researchers argue that existing data protection regulation has many unintended consequences that lead to negative political side-effects. For example, data protection

principles can easily be captured by internet organizations. Especially the reliance on notice-and-choice often legitimizes data collection and could lead to a responsibilisation of individuals for collective risks of surveillance (Hull 2015; Hartzog 2017; Matzner et al. 2016). Rather than mobilizing instruments and normative principles against disruptive practices of contemporary surveillance economies, some critiques suggest that current data protection regulation could be understood as an alley of surveillance for these reasons (Bennett/ Raab 2003; Coll 2014).

However, although these various challenges are obvious, it can seriously be questioned if the recent development of the General Data Protection Regulation (GDPR) can address the mentioned issues in an appropriate way. Generally, it can be argued that the GDPR provides no significant conceptual development regarding the core principles and goals of data protection (Zarsky 2017). On the contrary, as several critiques suggest, it can be expected that the GDPR does not lead to a more sufficient data protection regulation (Roßnagel 2016). For example, providing conditions for informational self-determination in terms of individual control or the goal of protecting personal information still remain the core aspects of data protection in the GDPR, although they can be questioned in a myriad of ways (Koops 2014).

Consequently, we argue that developing data protection only by enforcing existing normative data protection principles and regulatory techniques is not sufficient. However, abandoning established data protection instruments and principles completely is also inappropriate (Hartzog 2017). In order to think about alternatives to these two options, we argue for a *reinterpretation* of data protection as well as for the development of new institutions and regulatory techniques that could provide a basis for data protection for the networked society. Although there are various calls for reinventing data protection in other directions by taking new sociotechnical developments and contemporary user practices seriously (Ladeur 2015; Etzioni 2015), there is still a lack of an appropriate blueprint for data protection than can deal with the mentioned challenges in an appropriate way (Hartzog 2018).

The following considerations aim at providing a conceptual foundation for moving data protection in other directions. In this context, we argue for emphasizing the role of trust in relation to issues of data protection. Generally, we understand trust as a normative expectation that is related to the fulfillment of specific responsibilities. In this context, we argue that trust related phenomena always entail an explicit or implicit expectation that others should act upon presupposed collective practices and norms. Instead of using a concept of trust that primarily focuses on individual actions and decisions of trustors as suggested by Luhmann (2001), we argue for using an understanding of trust that focuses on the reproduction of normative expectations that are grounded in social practices (Walker 2006). In relation to informational privacy, the expectation that organizational actors such as

service providers or other users are dealing with the data according to specific presupposed societal norms of trust is of central importance in this regard (Nissenbaum 2010). By taking a normative understanding of trust seriously, data protection is not about providing individual information control or only about protecting individuals. Rather it is about protecting social relations of trust on the basis of shared informational norms (Sloan/ Warner 2014; Waldman 2018). In this paper, we discuss the consequences of using trust as a normative reference point. In this regard, we follow recent considerations that stress the important role of trust in relation to data protection (Eichenhofer 2016; Richards/ Hartzog 2016; Hartzog 2018; Martin 2013; Waldman 2018). Whereas these considerations focus on different aspects of trust regarding challenges of data protection, they agree that recognizing trust is central for providing fundamental shifts in data protection. In this regard, trust not only provides an alternative to the paradigm of privacy as individual control (Eichenhofer 2016), but also gives new directions for reinterpreting existing data protection principles of transparency or regulatory techniques such as informed consent (Richards/ Hartzog 2016). Furthermore, the development of new institutions and regulatory techniques can be guided by using the trust category as a normative reference point. For example, the relevance of information fiduciaries that are responsible for controlling organizational practices of data use or independent organizations that are obligated for controlling the compliance with informational norms are central in this regard (Balkin 2016). However, although these considerations provide a good starting point for thinking about data protection in terms of trust, they often do not provide an appropriate theoretical understanding of trust. In particular, especially the normative and collective foundation of trust phenomena is often not elaborated sufficiently. Furthermore, specific challenges of trust constitution like the reproduction and the development of informational norms are often not systematically discussed in relation to various regulatory techniques. In this regard, we not only bring current research regarding trust and data protection together, but also discuss the implications of taking trust seriously for data protection. In addition, we provide some conceptual clarifications regarding questions of trust constitution as well as develop criteria for establishing an institutional design that provides conditions for normative justifiable trust in relation to challenges of data protection.

Our paper is structured as follows. We begin by giving a short overview of the current data protection regulation by referring to the GDPR. Then in the next section we introduce the trust concept as a starting point to move data protection in another direction. After elaborating our understanding of trust, we outline the consequences of using the trust category for data protection, followed by providing examples for an institutional design that answers these challenges. In this context, we argue for information fiduciaries and the

institutionalization of independent organizations. Our conclusion along with further challenges for prospect studies are provided in the final section.

2. Challenges of data protection and the General Data Protection Regulation

The regulatory approach of the GDPR aims at strengthening the rights of individuals by "reinforcing the obligations and responsibilities of data controllers through a directly enforceable hard law-tool in the form of an EU Regulation." (Pagallo 2017: 40) In this context, the GDPR regulation primarily rests on data protection principles like individual consent, data minimization, purpose limitation, integrity and confidentiality as well as norms of fairness, lawfulness and transparency of data processing. The provisions of the GDPR are reiterations of established legal concepts, which are already stated in the European data protection law (Zarsky 2017: 1004). The rationality of using strict data protection principles for governing regulation of data processing rests primarily on the idea that data processing organizations cannot be trusted to develop these rules on their own. Therefore, the dominant approach can be described in terms of a classical command-and-control regulation that rests on strong legal rules and tools of sanction that are mobilized in case of non-compliance with legal rules (Yeung 2017: 36 f.). However, although this rationality of regulation seems intuitive at a first glance, its appropriateness can be questioned in a myriad of ways: as various critiques convincingly suggest (e.g., Mayer-Schönberger/ Padova 2016; Roßnagel 2016; Zarsky 2017), the GDPR is incompatible with recent sociotechnical developments of big data. In particular, the rationality of big data contradicts almost all data protection principles. For instance, the principle of purpose limitation rests on the notion that personal data must be collected for a specific, explicit, and legitimate purpose, which has to be specified at the time of collection. On the contrary, big data is about using data in ways that neither the collecting entities nor the data subjects considered at the time of collection (Hirsch 2014: 391; Zarsky 2017: 1006). Another cornerstone of the GDPR is the reliance on the data minimization principle. In this context, the GDPR states that data must be "limited to what is necessary in relation to the purposes for which they are processed."[1] Obviously, the data minimization principle contradicts with practices of big data. For example, believers in data science hold on to the promise that collecting as much data as possible is needed to gain greater knowledge. If data protection law is primarily understood as an instrument that is mobilized in order to prevent harm through restricting data collection and information flows on the basis of data minimization, we question how the potential risks as well as the potential benefits of big data that occur at a later stage of data use can be appropriately regulated. In other words, the function of data protection as an instrument that restricts rather than the one

[1] GDPR art. 5(1)(C).

that enables data processing is emphasized in the current GDPR. Therefore, it can be argued that current data protection has an inherent communication problem, because it is often seen as a barrier for organizations (Koops 2014: 258). Furthermore, enabling informational self-determination through more transparent and explicit consent is another objective that the GDPR aims to enforce. Here the underlying idea is that data subjects should be enabled to make more conscious and autonomous choices about the processing of their data by making informed consent more transparent (Schermer et al. 2014: 172). However, it is questionable if such developments can solve the often mentioned crisis of consent (Hull 2015; Schermer et al. 2014). Most obviously, assuming that individual information could be enabled through notice-and-choice is not only quite unrealistic, but also leads us to doubt the assumption that Internet services are used on the basis of autonomous choice, given the fact that Internet organizations are providing central infrastructures for sociality. Often users do not have other choices than signing up for and using a specific service (Roßnagel 2017: 18). Furthermore, as risks and potentials of big fata occur on the stage of data use, relying on explicit consent on the basis of decisions on the stage of data collection is not feasible anymore (Colonna 2014: 314). Although it is obvious that notice-and-choice fails to regulate big data, the failure could be described as a “successful failure” (Hull 2015) from the perspective of digital surveillance economies. That is because the reliance on notice-and-choice helps producing the fiction of an autonomous decision subject (Hull 2015). Individual information control is not only an opportunity, but also an obligation that is put on the shoulders of individual users. Therefore, externalizing privacy risks to individuals is an unintended consequence of an understanding of informational self-determination in terms of individual information control (Hartzog 2017).

Furthermore, the GDPR aims at protecting personal information that is directly linked to individuals (Taylor et al. 2017: 5). As Article 2 suggests, the “regulation applies to the processing of personal data.” Consequently, the GDPR excludes data that does not comply with the criteria of personal information from the impact of the law (Costa 2016: 143). For instance, in order to make big data possible, the GDPR legitimizes corresponding big data analysis by using pseudonomization techniques such as tokenization or scrambling, which will not allow the identification of unique data subjects (Zarsky 2017: 1011). However, doubt emerges whether protecting and avoiding personal identifiable information can be the main objective of data protection. Various critiques argue that relying on regulating personal information does not capture the central challenges of big data (Mantelero 2016; Pohle 2016). On the contrary, it can be assumed that most of the relevant impacts of big data analysis are outside the scope of the data protection law. For instance, automated decision making of big data can produce discriminatory effects on data subjects without using any personal identifiable data (Amoore 2014). Big data analysis is often not interested in

identifying specific individuals but rather intent on apprehending people in large amounts of fragmented data. In this context, the inferred meanings of statistical big data analyses have implications for people that have never agreed for using a specific Internet service. Even if we would imagine perfect informational self-determination or anonymity (which does not exist), big data analysis could have an impact on specific life chances. For instance, groups of individuals can be discriminated through algorithmic decisions based on ethical, gender or political bias (Amoore 2014; Matzner 2014; Mantelero 2016). Consequently, as recent considerations suggest, protecting networks and groups of individuals becomes more and more the condition for protecting individuals (Costa 2016: 144; Floridi 2017: 98).

Another fallacy that is stated regarding the GDPR is the fact that data protection is primarily understood in terms of regulating data processing. Therefore, the challenges concerning the actual sociotechnical design of information technologies are not appropriately addressed either. Especially issues of deceptive design of information technologies or underlying ethical biases that influence algorithmic decision making have an impact on privacy, whereas these challenges go beyond issues of merely regulating data processing (Hartzog 2018; Wachter et al. 2017). Although the GDPR focuses on establishing the privacy by design approach that aims at implementing data protection principles into technologies, it can also be questioned if the current legal approach can deal with the challenges regarding the design of information technologies. For instance, obligations of privacy by design are only related to data collectors, whereas the concrete producers of information technologies are not addressed. In this context, one could be skeptical regarding the scope of the privacy by design approach that is established in the GDPR (Roßnagel et al. 2016: 174). Yet, not only is the concrete design of information technologies relevant, the design of organizational practices also plays a critical role for data protection as well. In this regard, some critiques argue that the GDPR risks reproducing a gap between the law preached in the books and concrete organizational practices that take data protection seriously. This is because the regulation rests too much on fulfilling abstract norms without asking how to reproduce these norms in the context of concrete organizational practices (Koops/ Leenes 2013; Koops 2014). Therefore, the current practice of "filling in forms about compliance with rules runs the risk that rules are blindly followed in their letters, but that their spirit is overlooked: the spirit of data protection can hardly be captured in documentation." (Koops 2014: 255)[2]

Yet, not only sociotechnical developments are challenging established data protection principles and instruments, user practices are also challenging the normative assumptions

[2] For instance, conducting an appropriate privacy impact assessment and translating the findings into a privacy friendly design as suggested in Article 23, requires an attitude that goes beyond merely compliance with abstract legal rules and that understands the logic behind abstract data protection principles (Koops 2014: 255).

and core principles of data protection (Ladeur 2015; Stalder 2011). As empirical studies concerning user practices suggest (e.g., Barth 2016; Marwick/ boyd 2014; Ochs/ Büttner 2018), the dominant technique for establishing privacy in the networked society is not through restricting or controlling information flows. Given that contemporary sociality and subjectivity is constituted through sharing a lot of information, users establish techniques to achieve privacy in spite of data intensive practices. For instance, more recent empirical evidence suggests that users try to achieve privacy by delegating trust to service providers (Ochs/ Büttner 2018: 62 f.). Whereas it can be questioned if this act of delegation can be grounded on normative justifiable trust, techniques of delegation suggest a way to achieve privacy beyond individual information control.[3]

Taking these outlined critiques seriously implies that the future of data protection cannot rest on the idea of improving existing principles and techniques of data protection on the basis of normative ideas like privacy as individual information control. In the following section, we argue that a reinterpretation of data protection is necessary in order to deal with these challenges. Before we discuss the role of the trust category for dealing with these challenges, we summarize some criteria for data protection for the networked society: First, as the crisis of consent and challenges of big data suggest, there is a specific need for providing sufficient data protection without relying on explicit notice-and-choice, while enabling accountable and ethical big data use (Cate et al. 2014; Mayer-Schönberger/ Padova 2016: 332). In this context, data protection has to address the collective risks of data processing that go beyond protecting individuals or personal information. Second, data protection cannot only be about restricting information flows. Especially the promises of big data as well as data intensive practices of users suggest that data protection cannot primarily be understood as an instrument that is mobilized against big data. On the contrary, we have to ask for data protection that functions *in spite* of data intensive practices (Ochs/ Büttner 2018: 73). Third, challenges that go beyond data processing like the design of information technologies and organizational practices are also of great importance. We can address these challenges of data protection only by having an appropriate normative reference point that guides the search for alternative options for data protection.

3. The role of trust for moving data protection forward

In this section, we discuss the relevance of considering the trust category to push the data protection discussion in a new direction. First, we present the theoretical foundations of trust,

[3] As some authors suggest, this trust in service providers is based on the fact that a huge amount of users are using services like Facebook. This “law of large numbers” as well the fact that disruptive data processing is often not perceived justifies trust (Ochs/ Büttner 2018: 63; Morton 2014).

where we argue that only an understanding of trust that takes the normative and collective foundations of trust seriously is able to provide a sufficient starting point to address challenges of data protection. Then, we discuss the implications of using the trust category for the development of data protection. In order to show the added benefit of using trust as a normative reference point for the discussion of data protection, we refer to the critical remarks that we have made in Section 2.

3.1 Trust: theoretical foundations:

Although a broad spectrum of research on trust exists, there is still a lack of agreement concerning a theoretical conceptualization of trust. However, there are some core issues and assumptions that are broadly shared in trust research. Generally, many considerations agree that the term trust refers to some kind of positive expectation concerning the actions and intentions of others (e.g., Möllering 2001: 404; Offe 2001: 249). In situations of trust, we expect that others take our expectations into account, irrespective of the ability to monitor or control the actions of others. Therefore, trust always implies some form of delegation of responsibility and control from a trustor to a trustee (Kohring 2011). In relation to this act of delegation, it is often argued that trust inherently involves the possibility to become vulnerable to the actions of others (Mayer et al. 1995: 712). Though trust involves some risks of vulnerability, it allows the trustor to act with freedom. In this context, many theories understand trust in a functionalistic sense and argue that trust is necessary for dealing with social complexity (Lewis/ Weigert 1985; Luhmann 2000).

Whereas these assumptions are more or less shared by many trust theories, various theoretical considerations focus on different core aspects of the trust phenomenon (Kohring 2011). In this regard, some theories primarily focus on the individual actions and perceptions of trustors. These considerations aim at clarifying the term trust by asking for a specific kind of action that is constitutive for trust related phenomena. Here, theoretical approaches that understand trust in terms of individual risk management are relevant (Luhmann 2001; Sztompka 1999). For example, according to Niklas Luhmann (2001: 149), we can only speak of trust, if actors are able to reflect and perceive the specific risks that are related to trust based decisions. Thus, if actors only have positive expectations about the future without having the opportunity to make individual decisions for specific actions, they take a position of confidence, not of trust. Looking at trust from this perspective, the opportunity to decide for specific actions on the basis of perceived risks is constitutive for actions of trust. Yet, trust is not only about making decisions on the basis of perceived risks but also about dealing with risks *as if* they were not problematic (Lagerspetz 2015: 29). In other words, the function of

trust based actions is establishing positive expectations about the future by suspending perceived risks (Möllering 2006).

Although a perspective on trust as individual risk management provides a starting point to distinguish trust from a phenomenon such as confidence, solely focusing on individual decisions of the trustor is inappropriate for clarifying the trust phenomenon for various reasons: Firstly, an account of trust as individual risk management can be challenged from a normative perspective. Understanding trust only in terms of individual decisions of the trustor indicates that problems of trust are primarily perceived from the perspective of the trustor, whereas questions regarding the trustworthiness of the trustee are not taken into account (Meijboom et al. 2006). Therefore, a specific theoretical understanding of trust has consequences on how problems of trust are framed and what will emerge as a problem of trust. For example, by applying an understanding of trust as individual risk management to challenges of data protection, the focus is on providing conditions for individual risk management. In this regard, complex use-agreements are perceived as a primary hurdle for the trust constitution, because they prevent users from making informed trust decisions. Therefore, we can understand the development of regulatory approaches that primarily aim at informing users about specific privacy risks that are related to the use of a specific Internet service as trust building strategies (Basu et al. 2016; Jandt 2008; Pieters 2011). However, it is obvious that such an understanding of trust has no additional benefit to move data protection in another direction. On the contrary, it implies a reiteration of approaches that try to achieve privacy by primarily focusing on providing explicit consent for better autonomous decision making. In this context, only focusing on providing conditions for individual risk management does not only put the burden of trust on the shoulders of the individual trustor, but also tends to neglect the role of the trustee for meeting specific obligations and responsibilities that justify the trust that the trustor delegates to the trustee. For example, informing users in a more transparent way about privacy risks that they can make informed decisions does not necessarily imply that organizations are trustworthy themselves. For these reasons, by using an understanding of trust as individual risk management, the social interaction between trustor and trustee can be entirely absent (Meijboom 2008: 68). Secondly, we can also challenge the assumption that individual decisions on the basis of perceived risks are a constitutive element of trust from a socio-theoretical perspective. Often, we have no awareness about the fact that we ground our actions on trust, until our trust expectations are disrupted. In other words, mostly we trust implicitly without perceiving or assuming any risks (Endreß 2001: 177; Walker 2006: 78). Yet, this does not imply that risks are not a central element of trust related phenomena. On the contrary, the risk to be vulnerable to the actions of others is a constitutive element for trust, but it can be questioned whether individual decisions based on a perception of risks are mandatory elements for

defining trust (Endreß 2010: 99). Thirdly, reducing the trust phenomenon to individual decisions neglects the fact that trust always involves normative expectations that are implicitly presupposed in collective practices. The fact that trust is inherently related to normative expectations becomes obvious in situations where breaches of trust occur. In these situations, we are prepared to react negatively and hold others responsible for breaching our presupposed expectations (Holton 1994). Because the legitimacy of disappointed expectations of trust is not even questioned after a breach of trust, such expectations can be characterized as normative expectations. In turn, having normative expectations implies holding others accountable for meeting specific obligations. In other words, "[i]n trusting one has *normative expectations* to others, expectations of others that they will do what they should and hence that we are entitled to hold them to it […]." (Walker 2006: 80, emphasis in the original text; Hawley 2014: 8). Because trust expectations are related to presumed collective practices, they cannot be reduced to individual perceptions or decisions (Endreß 2001).

Taking this normative component of trust seriously, we argue that trust related phenomena always entail some kind of normative expectations that are related to the fulfillment of specific responsibilities. By bringing normative expectations to the fore, we can argue that trust is not mere reliance or an anticipation of the actions of others based on positive expectations. Even if we lack reasons that others act according to our trust expectations, we expect that others should do something and hold them accountable for disrupting normative expectations (Walker 2006: 69). For instance, we do not know for sure if organizations use our data in a responsible and normatively acceptable way. On the contrary, we have good reasons to be skeptical. However, when we are sharing personal information we have normative expectations that our information is being used according to normative principles and react negatively when we are, for instance, discriminated on the basis of organizational decisions (Nissenbaum 2010; Waldman 2018: 69). In this context, it makes sense to use the notion of trust even if the various actors that are controlling and using data cannot be specified in advance. In other words, knowing other actors and their intentions is not necessary for having trust expectations, which is often the case in complex institutionalized infrastructures. For instance, the fact that we are prepared to react negatively in the case of poor service offered by an airline shows that our reliance is based on normative expectations. Therefore, our reliance on complex institutions is based on trust that assumes the responsibility of others (Walker 2006: 85).

Furthermore, the outlined considerations imply that accepting and acting according to normative expectations by others is not a necessary condition for having normative

expectations regarding the actions of others.[4] Therefore, it is plausible to make sense of trust expectations even if there is a good reason to be skeptical about these expectations being met by other actors. However, if normative expectations and responsibilities for meeting specific obligations are unclear and widely contested, we cannot presuppose the conditions for *trust relationships*. On the one hand, it can be argued that normative expectations regarding an appropriate data use are of central importance, while on the other hand the conditions for thinking about the relation of users and Internet organizations in terms of a trust relationship are not necessarily fulfilled. In order to presuppose a trust relationship, there is a specific need that other actors accept normative expectations and that we can hold them accountable for breaching the norms of trust (Kohring 2011). In this context, we can suppose that appropriate conditions for trust cannot be presumed in relation to current data protection. This is because appropriate norms for actual data use cannot be presupposed for instance. There is a lack of informational norms that are appropriate for regulating the benefits as well as the risks of big data (Ladeur 2015; Sloan/ Warner 2014). Furthermore, the responsibilities for dealing with challenges of big data and privacy related risks are not well distributed either. The fact that the responsibility for dealing with privacy risks is often delegated to individual users reveals that organizations are not held accountable. Furthermore, users are often not aware when their trust is breached (Richards/ Hartzog 2016; Mantelero 2016). The fact that breaches of trust in the case of inappropriate data use often remain undetected also implies that sanctions for breach of trust are not mobilized. Beyond this, as users have to accept the disruption of normative expectations by accepting informed consent (Barocas/ Nissenbaum 2014: 65), we can be skeptical about the trustworthiness of Internet organizations.

Therefore, we understand problems of trust as challenges concerning the reproduction of normative expectations and collective distributed responsibilities. We argue that sufficient conditions for trust constitution in the context of data protection are not fulfilled until it is not possible to presuppose appropriate informational norms and an institutional infrastructure that provides conditions for reproducing and controlling the fulfillment of the corresponding informational norms. Following these conjectures, we argue that we cannot presuppose conditions for trust relationships with regard to Internet organizations. Instead, we understand trust as a result of appropriate processes of institutionalization (De Paoli et al. 2011).

[4] This argument is made by Meijboom (2006: 170): „[T]he acceptance of trust by the trustee is not a necessary condition for someone's moral expectations. My belief that an adequate food safety system is something that can be expected of the government is not depending on whether my expectations are explicitly accepted. I consider myself entitled to expect this."

3.2 Consequences of a trust perspective for data protection

In this subsection we will argue that using a normative and sociologically influenced understanding of trust is of central importance to think about new directions of data protection. While we refer to the critical remarks of Section 2 concerning the current development of data protection, we discuss the consequences of taking trust seriously in data protection regulation. Generally speaking, the current interest for dealing with the trust category regarding data protection and privacy challenges is also highly related to the crisis of privacy as individual information control. Thus, it is not surprising that various authors argue that the trust category can provide a viable alternative to the paradigm of individual information control (Eichenhofer 2016; Hartzog 2018; Richards/ Hartzog 2016; Waldman 2018). As outlined, a central argument for taking trust into account refers to the fact that individual informational control becomes more and more unrealistic in times of data intensive practices. Against this backdrop, there is a specific need for delegating responsibility and control to data collectors and external entities that are obligated for controlling data use practices in organizations. Trust always implies an act of delegation of control and responsibility to other actors (Kohring 2011). Thus, the recognition of the trust category offers an analytical starting point to think about regulatory alternatives to the paradigm of individual information control (Eichenhofer 2016: 51). However, trust is not only of interest because individual information control is no longer feasible. Furthermore, recognizing trust in relation to privacy and data protection implies that meeting normative expectations concerning the appropriateness of information flows is more important than the ability of individual information control. In most social contexts, we are sharing a lot of information without having the actual expectation of controlling such information flows by ourselves. The reason is that we implicitly trust that normative expectations concerning the appropriateness of information flows are recognized by other actors (Nissenbaum 2010; Richards/ Hartzog 2016). In this regard, the most relevant trust based expectation in relation to informational privacy is that information is not being shared indiscriminately. For example, we expect that health data is being shared with actors such as physicians that are responsible for dealing with our health issues. However, sharing health data without consent with an employer would not only be considered as a breach of privacy but also as a breach of contextual integrity which would be recognized as a breach of trust. This implies that privacy and trust go hand in hand in informational contexts (Richards/ Hartzog 2016; Waldman 2018).

If we understand privacy as trust in the appropriateness of information flows, various implications for thinking about privacy and data protection regulation emerge: as soon as questions regarding the appropriateness of information flows on the basis of trust norms are central, data protection regulation cannot primarily focus on restricting data collection. The

current approach of regulating all personal data processing from the moment of collection on the basis of notice-and-choice and data protection principles seems inappropriate from a trust perspective. Generally, the fact that data protection regulation aims at prohibiting all data collection expect those obtained with user consent implicitly suggests the lack of appropriate informational norms. Because we do not have informational norms that govern the actual data use related to normative expectations of trust, data protection regulation aims at regulating data collection primarily on the basis of notice-and-choice (Etzioni 2015: 25; Schermer et al. 2014: 180). However, a trust perspective implies that challenges of developing and reproducing informational norms cannot catch up by solely relying on data protection principles that are primarily mobilized in order to restrict information flows. Especially, the reproduction of normative trust expectations has to rely on concrete practices that cannot caught up solely on relying on abstract legal norms. In other words, we do not only have to trust in abstract legal norms, but also in concrete practices and decisions that are made in specific organizational contexts (Hartmann 2011; Offe 2001: 276). As we argued before (see Section 2), relying too much on regulating data processing through the lens of data protection principles can lead to an overestimation of norm compliance that risks overseeing the logic behind the many rules and underestimates the reproduction of concrete organizational practices. From a trust perspective, which we follow in this paper, the focus on concrete organizational practices becomes more relevant.

Furthermore, looking at the reproduction of informational norms and concrete organizational practices implies a shift from focusing on regulating data collection to regulating the actual data use. In this regard, various authors argue for a so-called “use-regulation” approach (Cate et al. 2014; Etzioni 2015; Ladeur 2015; Mantelero 2014: 655; Mayer-Schönberger/ Cukier 2013: 173 ff.). Those advocates of use regulation argue that the relevant risks and potentials of big data occur on the stage of the actual data use and cannot be determined prior to the point of collection. Therefore, there is a specific need for developing rules that govern the actual data use. From this perspective, focus on prohibiting data collection cannot be the answer in order to deal with the challenge of regulating information flows (Cate at al. 2014; Etzioni 2015: 19). Another argument that proponents of use regulation bring up is that use regulation implies holding organizations more accountable for data use practices. Yet, not only the reliance on individual consent, but also the establishment of appropriate organizational safeguards that guarantee normative justifiable practices of data use is relevant. In this context, Mayer-Schönberger and Padova argue:

> “While used-based regulation enables processing entities to engage in ethical and accountable uses of personal data without formal consent of the individual, it also saddles them with the explicit duty to deliberate assessment procedures *ex ante* – not just of the benefits but also the potential risks and harms for individuals associated with a particular

> data use – and the necessity to devise and implement concrete mitigation strategies." (Mayer-Schönberger/ Padova 2016: 332, emphasis in the original text)

As these considerations suggest, use-regulation provides a regulatory path option for data protection that does not only imply holding data organizations more accountable for mitigating privacy risks, it also opens up opportunities for regulating potentials benefits and risks of data processing. Therefore, use-regulation may provide an understanding of data protection that considers more the enabling rather than the restricting function of data protection. Furthermore, because use-regulation implies regulating data processing on the basis of informational norms, the above mentioned challenges of trust constitution regarding developing and reproducing normative expectations and practices are again of central importance. In this context, linking the discussion of use-regulation with considerations regarding trust constitution would be helpful in order to discuss the challenges that go along with a normative justifiable data use.

Furthermore, utilizing a trust perspective enables us to recognize the challenges of privacy, which are not adequately addressed by the current data protection law. Especially, we can understand ethical problems of discrimination that go beyond protecting individuals as breaches of trust norms. Therefore, because trust refers to implicit shared social norms that are grounded in social practices, recognizing trust for data protection implies protecting social relations rather than individuals (Waldman 2018: 69 f.).

However, the category of trust not only gives us new directions for data protection, but also provides us a promising starting point for an appropriate reinterpretation of established data protection instruments like notice-and-choice. While the argument that focusing on notice-and-choice puts an unrealistic burden on the individual is widely shared and convincing, it is often quite unclear what conclusions should be drawn from these critiques (Sloan/ Warner 2014; Hoboken 2016: 249). Using a normative understanding of trust can provide an alternative view on notice-and-choice that is able to avoid the pitfalls of current consent regime (Richards/ Hartzog 2016). From a trust perspective that takes the reproduction of informational norms seriously, the role of informed consent cannot solely be on determining the legitimacy of data processing and providing information about every data collection and use. In particular, if we focus on establishing and reproducing informational norms that govern data use, explicit consent for every data collection seems no longer feasible and necessary. If we could presuppose appropriate norms of trust for the regulation of the actual data use, then there would be no specific need to inform users about each and every data collection on the basis of explicit consent (Nissenbaum 2011; Schermer et al. 2014). Instead of informing users about every data collection and understanding transparency in providing as much as information as possible, taking trust seriously implies also a reinterpretation of

transparency. As Richards and Hartzog argue, we can grasp transparency in terms of honesty by using trust as a normative reference point:

> "But if trust is to be kept, it is not sufficient to be merely "open" or "transparent." Trust in information relationships requires an affirmative obligation of honesty to correct misinterpretations and to actively dispel notions of mistaken trust. […] Honesty […] requires more affirmative steps than passive notice, and includes an obligation to make sure that trusters are actually aware of things that matter to them. […] Honesty also serves the additional function of forcing companies to take stock of their information practices in order to be accurate when keeping individuals informed." (Richards/ Hartzog 2016: 462 f.)

This reinterpretation of transparency in terms of honesty implies that the central function of informed consent is to establish a normative justifiable trustworthiness of organizations. In this context, informed consent would be about informing users that organizational practices are recognizing specific norms of trust. Furthermore, providing appropriate conditions for trust would also imply that users are informed about breaches of trust. Yet, only if users are informed about trust breaches, trust can actually be justified. In other words, there is a specific need not only to inform users about the future usage of their data, but also about the specific data use practices that have already taken place (Wachter et al. 2017). While the current notice-and-choice regime is inappropriate for informing users, a trust perspective would understand notice-and-choice as an instrument that is necessary to avoid misplaced trust (Richards/ Hartzog 2016).

However, although this approach suggests some ways to move data protection in another direction, we can be skeptical about the possible negative implications. Critiques argue (e.g., Hoofnagle 2014) that use-regulation opens up the risk that organizations collect huge amounts of data and use it in expansive ways. Furthermore, it is argued that use-regulation implies a regulation that is paternalistic. While the control shifts from individual persons to organizations, some critics of the use-regulation approach fear that organizations will make decisions without recognizing the interests of users (e.g., Cavoukian 2015).

4. Regulatory approaches for constituting trust

In the following section, we provide exemplary regulatory approaches for an institutional design that takes the outlined challenges of trust constitution into account. We argue that challenges of reproducing, developing, and controlling the compliance of norms of trust require an institutional design that relies on a variety of different regulatory approaches. In this regard, we discuss the relevance of professions as information fiduciaries that are

responsible for ensuring normatively appropriate data use practices in organizations. Furthermore, we argue for institutionalizing independent organizations that are obligated for controlling the fulfillment of normative expectations and that are responsible for sanctioning breaches of trust.

4.1 Information fiduciaries

While taking trust seriously for issues of data protection, the question of the reproduction of normative appropriate practices of data use in the context of organizations is of central importance. As we argued before, only understanding data protection through the lens of regulating data flows with the help of established data protection principles runs the risk of reproducing a gap between codified law and concrete practices. Thus, in order to address these challenges, we discuss the relevance of information fiduciaries. In this regard, we refer to recent considerations that claim the importance of information fiduciaries in the context of data protection (Balkin 2016; Brennan-Marquez 2015; Richards/ Hartzog 2016; Waldman 2018: 88 ff.). The main goal of this section is to relate the core ideas of these works to the challenges of trust constitution.

In general, information fiduciaries are traditionally established in societal domains like law and medicine. We do not only trust lawyers and representatives of the medical profession regarding their specific expertise, we also trust that these professions are using our information in a discrete and loyal way (Richards/ Hartzog 2016: 457). Therefore, traditional professions could be understood as information fiduciaries that are obligated for meeting specific normative expectations regarding appropriate information flows. Yet, what does it mean to trust professions as information fiduciaries? In most cases, we do not have any kind of personal relationship to professions. Therefore, we cannot rely on personal familiarity in order to justify our trust. However, we can expect that these professions are obligated to follow ethical standards, which in turn are controlled by independent organizations like the physician association in the case of the medical profession. In other words, we can trust that professions respect our normative expectations regarding appropriate information flows because of the underlying normative infrastructure that professions are embedded in (Hartmann 2011: 285). How could these general considerations be applied to challenges of data protection? Although practices of data use of Internet firms like Facebook or Google seem quite different from classical information fiduciaries at first, there are nonetheless relevant structural similarities between classical professions and current Internet organizations (Balkin 2016: 1221). Firstly, the relationship between classical professionals and their clients as well as the relationship between Internet users and Internet organizations

is characterized by information asymmetries. That is, neither practices of professionals nor data use practices in organizations are transparent for outsiders in most cases. However, even if information about these practices would be available to them, it would not be possible to individually control the activities of information fiduciaries as well as Internet organizations. Furthermore, classical information fiduciaries as well as contemporary Internet organizations such as Facebook or Google serve relevant societal functions. Nowadays, we rely heavily on information fiduciaries and Internet organizations, as they provide central infrastructures for contemporary sociality. Thus, sharing information with them is a necessity (Balkin 2016: 1183; Brennan-Marquez 2015: 638; Waldman 2018) In other words, we have to trust practices of information fiduciaries and Internet organizations despite the fact that we often have no obvious reason to do so. Therefore, there is a specific need for constituting normative justifiable trust in practices of Internet organizations that can be implicitly presupposed like the trust in classical information fiduciaries (Balkin 2016: 1183).

Considering the relevance of information fiduciaries has direct implications for dealing with challenges of data protection. One of the most relevant merits of professions is that they act as representatives of their clients (Sanders 2014). In this context, information fiduciaries in data organizations would represent the users. This representation of users implies a delegation of responsibility for controlling information practices in organizations to information fiduciaries that leads to autonomy gains for users. Therefore, autonomy is not served through individual information control, but through an act of delegation of trust (Ochs/ Büttner 2018: 73). Taking information fiduciaries as user representatives seriously in data protection could counteract the overwhelming requirements that users are obligated for dealing with data protection issues. Furthermore, professions that act as information fiduciaries are of central importance for the reproduction of normative practices. Information fiduciaries are especially responsible for reproducing and linking abstract data protection principles to concrete practices (Vedder/ Naudts 2017: 14). Yet, practices of information fiduciaries go beyond merely norm compliance with data protection regulation. Generally, practices of professions follow ethical conducts that cannot be solely reduced to existing legal principles or legal contracts. Therefore, relationships to information fiduciaries cannot fully be explained in terms of contractual relations (Fitzgibbon 1999). For instance, in modern health care, patients maintain relationships to various actors from hospitals to health maintenance organizations to insurers. Hence, it would be impossible to describe privacy obligations on the basis of contracts and informed consent practices given the complexity of these relationships. The same is relevant for the relationship between Internet users and various Internet organizations that cannot solely be understood in terms of contractual relations (Balkin 2016: 1201; Nissenbaum 2011).

Also, if we understand the relationship between Internet users and Internet organizations on the basis of information fiduciary law instead of the law of notice-and-choice, this implies thinking about data protection as protecting relationships of trust. From this perspective, data protection is not an instrument that aims at separating users from Internet organizations (Waldman 2018: 88). On the contrary, talking and thinking about privacy and data protection in terms of trust implies that sharing information with Internet organizations is inevitable. Thus, we do not expect that no information is being used by Internet organizations. Also, we do not expect that every information that is being used can be translated into contractual obligations. Instead, we expect that information is being shared in a discrete and loyal way. Dealing with information in a discrete way is the main obligation of information fiduciaries (Richards/ Hartzog 2016). Therefore, strengthening accountability of data processors on the basis of information fiduciary law seems a relevant starting point in order to provide data protection in the networked society that puts the enabling as well as the restricting functions of data protection into consideration (Hartzog 2018: 105 f.; Waldman 2018: 88).

While these arguments for the institutionalization of information fiduciaries may be plausible in order to address challenges of data protection, there still remain some open questions. For instance, various critiques argue that relying on information fiduciaries runs risks of malpractice and paternalism. For instance, Cavoukian argues that focusing on regulating data use on the basis of information fiduciaries would have the effect

> "of weaken fundamental privacy rights of individuals, while strengthening the power of data users/ controllers to decide what personal data to collect and process, whenever and however they see fit, placing greater burdens on both individuals and regulators to seek effective redress. I consider this a paternalistic approach to privacy." (Cavoukian 2015: 294)

In this regard, Cavoukian (2015) fears a high potential of malpractice when responsibility is primarily delegated to information fiduciaries that act as data controllers in organizations. We agree that this argument is convincing, if we cannot presume appropriate informational norms and institutionalized safeguards. However, by taking the institutionalization of a trust infrastructure that can deal with the challenges of guaranteeing an appropriate data use seriously, we think that risks of malpractice can be mitigated. Furthermore, the argument that use regulation on the basis of information fiduciaries implies paternalism is implicitly based on the idea that only informational self-determination on the basis of individual information control can strengthening user autonomy. Delegating control from users to powerful organizations runs the risk of putting users under tutelage. However, while we should seriously consider the possibility of malpractice, the argument that relying on information fiduciaries inherently implies paternalism can be challenged by considering the role that trust

plays in relation to current user practices. Following the assumption that users already delegate trust to service providers (Büttner/ Ochs 2018), we can question whether the argument of paternalism in relation to information fiduciaries is still plausible. In this context, taking the trust of users in professional practices seriously would put the reciprocal nature of the relationship between information fiduciaries and users to the fore. In other words, considering information fiduciaries solely in terms of paternalism is an implication of understanding fiduciaries only as a unilateral relation from the point of view of the professional. In addition, this understanding is a consequence of neglecting the role of trust that clients delegate to professionals (Zaner 1991: 46).

Furthermore, it remains an open question what kind of actors should actually constitute information fiduciaries. Is there a specific need for developing new professions that combine ethical, legal, and technical expertise or is it more appropriate to assume various professions that are obligated to deal with the challenges of data protection? Although information fiduciaries could address some challenges of trust constitution, however the sole reliance on them is not enough for constituting normative justifiable trust. We can only grant trustworthy organizational practices if disruptive organizational practices could be made transparent. Furthermore, there is a specific need for effective sanctions in the case of data breaches. Another challenge we face is the development of appropriate norms that we can generally presuppose. If we cannot presuppose appropriate informational norms, also the normative expectations and responsibilities for information fiduciaries are unclear. From this perspective, we have to ask for institutional structures and regulatory techniques that control normative principles of data protection, which are obligated to sanction data breaches and that allow the development of new regulatory norms for data protection. As we will outline in the next paragraph, the institutionalization of intermediary organizations is necessary in order to address these challenges.

4.2 Intermediary organizations

While talking about intermediary organizations, we can think about nongovernmental organizations (NGOs), product testing organizations such as Stiftung Warentest, or supervisor organizations in the field of financial or environmental regulation such as the Financial Service Authority (FSA). Generally, intermediary organizations are directly located between regulators and regulatory targets. They are of central importance for constituting normative justifiable trustworthiness of regulated organizations. For instance, intermediary organizations are often obligated to control the compliance of regulatory standards and make breaches of regulatory norms transparent. In this context, they can enforce rules by

disclosing noncompliance with regulatory rules or by withdrawing relevant certifications. Furthermore, the translation of regulatory goals into practical forms that are useful for regulatory targets is another responsibility credited to intermediary organizations (Abbott et al. 2017: 7)

If we consider intermediary organizations in the field of data protection, there are some arguments for institutionalizing independent supervisor organizations that are responsible for controlling and estimating data protection risks (Mantelero 2016: 252; Regan 2017). For instance, current considerations argue for auditing of algorithms carried out by external regulators (e.g., Tutt 2017). The implied auditing processes go beyond merely rendering the code of an algorithm transparent. Instead, it is about auditing the decision-making processes of algorithms. Unpacking ethically problematic decisions or detecting discrimination is the central goal of such auditing (Mittelstadt et al. 2016: 13). Auditing processes are necessary in order to gain knowledge about specific risks concerning data use in various contexts. This knowledge is of central importance in order to develop new normative principles that can then guide ethical practices of data use (Ladeur 2015; Vedder/ Naudts 2017). Yet, establishing accountability of data organizations on the basis of auditing processes is not only about ex-post measures of algorithmic decision making. Furthermore, establishing mechanisms of accountability for data organizations aims at establishing an institutional design in which data organizations are liable without fail. The latter means holding Internet organizations not only accountable when privacy breaches occur, instead they have to prove that they take necessary actions in order to mitigate potential risks for data protection (Costa 2012). In other words, holding data organizations accountable by intermediary organizations implies that they are obligated to prove that their organizational practices are trustworthy.

Of course, there is a specific risk that this demonstration of trustworthiness works as a simple PR mechanism. Therefore, there is a specific need for regulatory instruments that guarantee normative justified trustworthiness. In this regard, we see institutionalized binding processes of certification as central importance for constituting public trustworthiness of data organizations. Intermediaries would proof if organizations institutionalize appropriate precautionary mechanisms for the use of risk technologies. Organizations that meet regulatory goals would receive a certificate from the supervisory organization (Will 2015, 12). An institutionalization of mandatory certification mechanism does not primarily understand the challenges of trust in providing conditions for individual trust decisions on the basis of informing users about privacy risks. Instead, it is about establishing normatively justifiable trustworthiness of data organizations, which are controlled by independent organizations (Bile et al. 2018: 98; Meijboom et al. 2006: 432). Of course, these considerations regarding binding certification mechanisms are anything but new. In the literature, the relevance of

institutionalizing independent audits is discussed for over two decades now (e.g., Roßnagel 1997). However, mandatory certification mechanisms are not implemented in data protection regulation so far. Also, the GDPR does not envisage binding certification mechanisms either. Furthermore, established auditing processes are often oriented in controlling the compliance with existing data protection principles. For these reasons, one could be skeptical if the GDPR is able to create incentives for a continuous improvement of data protection practices in organizations (Bile et al. 2018: 95).

Furthermore, justified trustworthiness on the basis of certification mechanisms can only be guaranteed if breaches of trust could actually be sanctioned. In this regard, noncompliance with regulatory norms could be sanctioned by withdrawing certifications or by paying fines. The main goal of institutionalizing mechanisms of sanctioning is enforcing conditions for compliance with regulatory norms. If mechanisms of sanctioning are not effective or if noncompliance with regulatory rules cannot be detected, the question emerges whether data organizations orient their practices regarding regulatory standards (Will 2015: 12).

Lastly, the legitimacy and trustworthiness of regulatory techniques depends largely on how noncompliance with regulatory standards can be made transparent by intermediary organizations (Will 2015: 12). Transparency regarding noncompliance with regulatory standards is especially relevant in the case of data protection regulation. Often, disruptions of privacy and trust occur beyond daily experience. In comparison to societal contexts where the materialization of risks is quite obvious such as the use of nuclear power, the use of big data technologies can generate risks that are often hidden (Helm 2016: 144; Mantelero 2016: 251). From this perspective, there is a specific need for transparency mechanisms that are appropriate for informing the public concerning data breaches. However, constituting transparency regarding data use practices in organizations is faced with serious challenges. For instance, trade secrecy law can justify hiding practices of data use in Internet organizations as well as decision making of algorithms (Pasquale 2015). In this context, how to establish transparency regarding data breaches without violating trade secrecies is a question of central importance. As Cohen (2012: 237) argues, other areas of society have developed regulatory techniques that can deal with this challenge in an appropriate way. For instance, the Financial Service Authority (FSA) acts as a financial supervisory organization that is obligated to make noncompliance with regulatory norms transparent without violating trade secrecies at the same time (Black 2003: 30).

Making disruptions of regulatory norms transparent is not a condition for establishing trust in regulatory techniques. Informing the public regarding breaches of trust is also different compared to the current mechanisms of informing users about noncompliance with data protection standards. Indeed, users have a right to be informed about data use practices in

organizations. However, due to power imbalances, few are motivated to initiate legal action when needed (Mayer-Schönberger 2010). Therefore, instead of proposing mechanisms of transparency that aim at informing individual users, we argue for ones that help constituting a critical public regarding data protection challenges. In this context, challenges of trust constitution have to deal with questions concerning the establishment of communicative and adaptive trust relations. From this perspective, relations of trust are always democratic and the democratic legitimacy of regulatory techniques depends on how conflicts can be delivered to public control (Kohring 2011: 281; Ochs/ Lamla 2017).

Taken together, we argue that intermediary organizations have different obligations for constituting trust. Constituting normative justifiable trustworthiness of organizational practices depends on binding certification that is conducted by independent organizations. In this regard, auditing processes are not relevant for testing the compliance with established data protection norms. The development of new knowledge concerning privacy risks that are related to big data is a necessary aspect of auditing processes. Furthermore, exercising sanctions by noncompliance with regulatory norms as well as informing the public regarding breaches of trust are central regulatory obligations of intermediary organizations.

5. Conclusion:

In this paper, we have outlined that the current data protection regulation face various challenges. While the GDPR rests on established data protection principles like data minimization and instruments like notice-and-choice, these approaches however cannot deal with the current socio-technical developments such as big data as well data intensive practices of users. Instead of developing data protection by solely improving existing data protection principles and instruments, we have argued for a reinterpretation of data protection and the development of new institutions. In this regard, we have discussed the relevance of trust as a normative reference point for moving data protection in another direction. While using an understanding of trust that takes the normative and collective foundation of trust seriously, we outlined the various implications for data protection. We argued that the trust category not only provides an alternative to the paradigm of privacy as individual information control, but also gives new directions for reinterpreting existing data protection principles. Furthermore, instead of controlling every instance of data collection primarily on the basis of a notice-and-choice approach, a trust perspective further implies a focus on regulating the actual data use practices in data organizations. In this context, the main challenge of trust constitution is the development of new informational norms that can guide the actual data use. These considerations suggest that data protection cannot rest on

formal legal rules or technological solutions. Rather, the challenges of trust constitution and data protection are about constituting a trust infrastructure that involves various actors and focuses on the distribution of various regulatory techniques. In this regard, we have discussed the relevance of information fiduciaries along with intermediary organizations. The former are of central importance to close the gap between formal legal rules and concrete data use practices. Furthermore, they also act as representatives of users. Intermediary organizations on the other hand are relevant in order to constitute trustworthiness of data organizations by enforcing external control through auditing processes and establishing binding certification. Providing sanctions as well as making disruptive data use practices in organizations transparent are also obligations of intermediary organizations.

Nonetheless, from our discussion there also emerged some questions for further research. Especially the concrete institutionalization of information fiduciaries and independent organizations are anything but clear today. Thus, it remains an open question, which actors constitute information fiduciaries and intermediary organizations. In this context, crosschecking regulatory challenges of data protection with regulatory challenges of other areas of society can be useful to guide processes of developing new institutions for data protection. Furthermore, a trust perspective implies a radical shift in data protection at some points. For instance, the current focus on informational self-determination in terms of individual information control is still the normative backbone of data protection. Therefore, a shift from a focus on regulating data collection to data use may contradict the corner stones of data protection. In this context, it is vital for future research to address questions regarding the potential of innovation that is established in the current data protection regulation.

References:

Abbott, Kenneth/ Levi-Faur, David/ Snidal, Duncan (2017): Introducing Regulatory Intermediaries. In: The ANNALS of the American Academy of Political and Social Science 670 (1), S. 6-13.

Albers, Marion (2017): Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen. In: Friedewald, Michael/ Lamla, Jörn/ Roßnagel, Alexander (Hg.): Informationelle Selbstbestimmung im digitalen Wandel. Springer, S. 11-36.

Amoore, Louise (2014): Security and the Claim to Privacy. In: International Political Sociology 1 (8), S. 108-112.

Balkin, Jack M. (2016): Information Fiduciaries and the First Amendment. In: UC Davis Law Review 49 (4), S. 1183-1234.

Barocas, Solon/ Nissenbaum, Helen (2014): Big Data`s End Run around Anonymity and Consent. In: Stodden, Victoria/ Bender, Stefan/ Nissenbaum, Helen (Hg.): Privacy, Big Data, and the Public Good. Frameworks for Engagement. Cambridge: Cambridge University Press, S. 44-75.

Barth, Niklas (2016): Kalte Vertrautheiten – Private Kommunikation auf der Social Network Site Facebook. In: Berliner Journal für Soziologie 25 (4), S. 459-489.

Basu, Anirban/ Marsh, Stephen/ Rahman, Mohammad Shahriar/ Kiyomoto, Shinsaku (2016): A Model for Personalised Percpetion of Policies. In: Habib et al. (Hg.): Trust Management X. 10th IFIP WG 11.11 International Conference. Proceedings, S. 52-62.

Bennett, Colin/ Raab, Charles (2003): The Governance of Privacy. Policy instruments in global perspective. Burlington: Ashgate.

Bile, Tamer/ Geminn, Christian/ Grigorjew, Olga/ Husemann, Charlotte/ Nebel, Maxi/ Roßnagel, Alexander (2018): Fördern und Fordern: Regelungsformen zur Anreizgestaltung für einen wirksameren Schutz von Privatheit und informationeller Selbstbestimmung. In: Friedewald, Michael (Hg.): Privatheit und selbstbestimmtes Leben in der digitalen Welt. Interdisziplinäre Perspektiven auf Herausforderungen des Datenschutzes. Wiesbaden: Springer, S. 83-126.

Black, Julia (2003): Mapping the Contours of Contemporary Financial Services Regulation. ESRC Centre for Analysis of Risk and Regulation.

Cate, Fred H./ Cullen, Peter/ Mayer-Schönberger (2014): Data Protection Principles for the 21th Century. Revising the 1980 OECD Guidelines. Online verfügbar unter:

https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf

Cavoukian, Ann (2015): Evolving FIPPs: Proactive Approaches to Privacy, Not Privacy Paternalism. In: Gutwirth, Serge/ Leenes, Ronald/ de Hert, Paul (Hg.): Reforming European Data Protection Law. Dordrecth/ Heidelberg/ New York/ London: Springer, S. 293-310.

Cohen, Julie E. (2012): Configuring the Networked Self. Law, Code, and the Play of Everyday Practice. New Haven/ London: Yale University Press.

Coll, Sami (2014): Power, knowledge, and the subjects of privacy: understanding privacy as the ally of surveillance. In: Information, Communication & Society 17 (10), S. 1250-1263.

Colonna, Liana (2014): Data Mining and Its Paradoxical Relationship to the Purpose Limitation Principle. In: Gutwirth, Serge/ Leenes, Ronald/ De Hert, Paul (Hg.): Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges. Dordrecht et al.: Springer, S. 299-322.

Costa, Luiz (2012): Privacy and the precautionary principle. In: Computer Law & Security Review 28 (1), S. 14-24.

Costa, Luiz (2016): Virtuality and Capabilities in a World of Ambient Intelligence. New Challenges to Privacy and Data Protection. Springer.

Eichenhofer, Johannes (2016): Privatheit im Internet als Vertrauensschutz. Eine Neukonstruktion der Europäischen Grundrechte auf Privatleben und Datenschutz. In: Der Staat 55, S. 41-67.

Endreß, Martin (2001): Vertrauen und Vertrautheit. In: Hartmann, Martin/ Offe, Claus (Hg.): Vertrauen. Die Grundlage des sozialen Zusammenhalts. Frankfurt am Main/ New York: Campus, S. 161-203.

Endreß (2010): Vertrauen – soziologische Perspektiven. In: Maring, Matthias (Hg.): Vertrauen – zwischen sozialem Kitt und Senkung der Transaktionskosten. Karlsruhe: Universitätsverlag, S. 91-114.

Etzioni, Amitai (2015): Privacy in a Cyber Age. Policy and Practice. New York: Palgrave Macmillan.

Fitzgibbon, Scott (1999): Fiduciary Relationships are not Contracts. In: Marquette Law Review 82 (2), S. 303-353.

Floridi, Luciano (2017): Group Privacy: A Defence and an Interpretation. In: Taylor, Linnet/ Floridi, Luciano/ van der Sloot, Bart (Hg.): Group Privacy. New Challenges of Data Technologies. Springer, S. 83-100.

Hagendorff, Thilo (2017): Das Ende der Informationskontrolle. Digitale Mediennutzung jenseits von Privatheit und Datenschutz. Bielefeld: transcript.

Hartmann, Martin (2011): Die Praxis des Vertrauens. Berlin: Suhrkamp.

Hartzog, Woodrow (2017): The Inadequate, Invaluable Fair Information Practices. In: Maryland Law Review 76 (4), S. 952-983.

Hartzog, Woodrow (2018): Privacy's Blueprint. The Battle to Control the Design of New Technologies. Cambridge et al.: Harvard University Press.

Hawley, Katherine (2012): Trust, Distrust and Commitment. In: Noûs 48 (1), S. 1-20.

Helm, Paula (2016): Group Privacy in Times of Big Data. A Literature Review. In: Digital Culture and Society 2 (2), S. 138-151.

Hirsch, Dennis D. (2014): The Glass House Effect: Big Data, The New Oil, and the Power of Analogy. In: Maine Law Review 66 (2), S. 374-395.

Hoboken, Joris van (2014): From Collection to Use in Privacy Regulation? A Forward-Looking Comparison of European and US Frameworks for Personal Data Processing. In: van der Sloot, Bart/ Broeders, Dennis/ Schrijvers, Erik (Hg.): Exploring the Boundaris of Big Data. Amsterdam: Amsterdam Press, S. 231-260.

Holton, Richard (1994): Deciding to Trust, Coming to Believe. In: Australian Journal of Philosophy 72, S. 63-76.

Hoofnagle, Chris Jay (2014): The Potemkinism of Privacy Pragmatism, Slate, 2. September: http://www.slate.com/articles/technology/future_tense/2014/09/data_use_regulation_the_libertarian_push_behind_a_new_take_on_privacy.html?via=gdpr-consent .

Hull, Gordon (2015): Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. In: Ethics and Information Technology 17 (2), S. 89-101.

Jandt, Silke (2008): Vertrauen im Mobile Commerce. Vorschläge für die rechtsverträgliche Gestaltung von Location Based Services. Baden-Baden: Nomos.

Kammourieh, Lanah/ Baar, Thomas/ Berens, Jos/ Letouzé, Emmanuel/ Manske, Julia/ Palmer, John/ Sangokoya, David/ Vinck, Patrick. In: Taylor, Linnet/ Floridi, Luciano/ van der Sloot, Bart (Hg.): Group Privacy. New Challenges of Data Technologies. Springer, S. 37-66.

Kohring, Matthias (2011): Zuversicht statt Vertrauen? Probleme der Vertrauenskonstitution in modernen Gesellschaften. In: Erwägen – Wissen – Ethik 22 (2), S. 279-282.

Koops, Bert-Jaap (2014): The trouble with European data protection law. In: International Data Privacy Law 4 (4), S. 250-261.

Koops, Bert-Japp/ Leenes, Ronald (2013): Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. In: International Review of Law, Computers & Technology 28 (2), S. 159-171.

Ladeur, Karl-Heinz (2015): Die Gesellschaft der Netzwerke und ihre Wissensordnung. Big Data, Datenschutz und die relationale Persönlichkeit. In: Süssenguth, Florian (Hg.): Die Gesellschaft der Daten. Bielefeld: transcript, S. 225-251.

Lagerspetz, Olli (2015): Trust, Ethics and Human Reason. London et al.: Bloomsbury.

Lewis, David J./ Weigert, Andrew (1985): Trust as a Social Reality. In: Social Forces 63 (4), S. 967-985.

Luhmann, Niklas (2000): Vertrauen. 4. Auflage. Stuttgart: Lucius und Lucius.

Luhmann, Niklas (2001): Vertrautheit, Vertrauen und Zuversicht. Probleme und Alternativen. In: Hartmann, Martin/ Offe, Claus (Hg.): Vertrauen. Die Grundlage des sozialen Zusammenhalts. Frankfurt am Main/ New York: Campus, S. 143-160.

Mantelero, Allesandro (2016): Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. In: Computer Law & Security Review 32, S. 238-255.

Martin, Kirsten (2013): Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online. In: First Monday 18 (12), Online verfügar unter: http://firstmonday.org/ojs/index.php/fm/article/view/4838/3802 .

Marwick, Alice E./ boyd, danah (2014): Networked privacy: How teenagers negotiate context in social media. In: new media & society 16 (7), S. 1051-1067.

Matzner, Tobias (2014): Why privacy is not enough in the context of "ubiquitous computing" and "big data". In: Journal of Information, Communication and Ethics in Society 12 (2), S. 93-106.

Matzner, Tobias/ Masur, Philipp K./ Ochs, Carsten/ von Pape, Thilo (2016): Do-It-Yourself Data Protection – Empowerment or Burden? In: Gutwirth, S./ Leenes, R./ De Hert, P. (Hg.): Data Protection on the Move. Current Developments in ICT and Privacy/ Data Protection (Law, Governance and Technology Series, vol. 24), Springer, S. 277-305.

Mayer, Roger C./ Davis, James H./ Schoorman, David F. (1995): An integrative model for organizational trust. In: The Academy of Management Review 20 (3), S. 709-734.

Mayer-Schönberger, Viktor (2010): Beyond Privacy, beyond Rights – Toward a "Systems" Theory of Information Governance. In: California Law Review 98 (6), S. 1853-1885.

Mayer-Schönberger, Viktor/ Cukier, Kenneth (2013): Big Data. A Revolution That Will Transform How We Live, Work and Think. London: John Murray.

Mayer-Schönberger, Viktor/ Padova, Yann (2016): Regime change? Enabling Big Data through Europe's new data protection regulation. In: The Columbia Science & Technology Law Review 17, S. 315-335.

Meijboom, Fanck (2006): Why increasing predictability cannot do the job alone when we aim to establish trust in the agri-food sector. Ethics and the politics of food. Wageningen: Wageningen University Press, S. 167-171.

Meijboom, Franck/ Visak, Tatjana/ Brom, Frans W. A. (2006): From trust to trustworthiness: Why information is not enough in the food sector. In: Journal of Agricultural and Environmental Ethics 19, S. 427-442.

Meijboom, Franck (2008): Problems of Trust. A Question of Trustworthiness. An ethical inquiry of trust and trustworthiness in the context of the agricultural and food sector. Dissertation.

Mittelstadt, Brent/ Allo, Patrick/ Taddeo, Mariarosaria/ Wachter, Sandra/ Floridi, Luciano (2016): The ethics of algorithms: Mapping the debate. Big Data & Society. 1-21.

Morton, Anthony (2014): "All my mates have got it, so it must be okay" : Constructing a Richer Understanding of Privacy Concerns – An Exploratory Focus Group Study. In: Gutwirth, Serge/ Leenes, Ronald/ De Hert, Paul (Hg.): Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges. Dordrecht et al.: Springer, S. 259-298.

Möllering, Guido (2001): The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation and Suspension. In: Sociology 35 (2), S. 403-420.

Möllering, Guido (2006): Trust: Reason, Routine, Reflexivity. Amsterdam et al.: Elsevier.

Nissenbaum, Helen (2010): Privacy in Context. Technology, Policy and the Integrity of Social Life. Stanford: Stanford University Press.

Nissenbaum, Helen (2011): A Contextual Approach to Privacy Online. DAEDALUS 140 (4), S. 32-48.

Ochs, Carsten/ Büttner, Barbara (2018): Das Internet als »Sauerstoff« und »Bedrohung«: Privatheitspraktiken zwischen analoger und digital-vernetzter Subjektivierung. In: Friedewald, Michael (Hg.): Privatheit und selbstbestimmtes Leben in der digitalen Welt. Interdisziplinäre Perspektiven auf aktuelle Herausforderungen des Datenschutzes. Wiesbaden: Springer.

Ochs, Carsten/ Lamla, Jörn (2017): Demokratische Privacy by Design. Kriterien soziotechnischer Gestaltung von Privatheit. In: Forschungsjournal Soziale Bewegungen 30 (2), S. 189-199.

Offe, Claus (2001): Wie können wir unseren Mitbürgern vertrauen? In: Hartmann, Martin/ Offe, Claus (Hg.): Vertrauen. Die Grundlage des sozialen Zusammenhalts. Frankfurt am Main/ New York: Campus, S. 241-294.

Oostveen, Manon (2016): Identifiability and the applicability of data protection to big data. In: International Data Privacy Law 6 (4), S. 299-309.

Pagallo, Ugo (2017): The Legal Challenges of Big Data. Putting Secondary Rules First in the Field of EU Data Protection. In: European Data Protection Law Review 3 (1), S. 36-46.

Pasquale, Frank (2015): The Black Box Society. The Secret Algorithms That Control Money and Information. Cambridge et al: Harvard University Press.

Pieters, Wolter (2011): Explanation and trust: what to tell the user in security and AI. In: Ethics Information Technology 13, S. 53-64.

Pohle, Jörg (2016): PERSONAL DATA NOT FOUND: Personenbezogene Entscheidungen als überfällige Neuausrichtung im Datenschutz. In: Datenschutz Nachrichten 1/2016, S. 14-19.

Regan, Priscilla M. (2017): Reviving the Public Trustee Concept and Applying It to Information Privacy Policy. In: Maryland Law Review 76 (4), S. 1025-1043.

Richards, Neil/ Hartzog, Woodrow (2016): Taking Trust Seriously in Privacy Law. In: Stanford Technology Law Review 19, S. 431-472

Roßnagel, Alexander (1997): Datenschutz-Audit. In: Datenschutz und Datensicherheit 21 (9), S. 505-515.

Roßnagel, Alexander (2016): Wie zukunftsfähig ist die Datenschutz-Grundverordnung? Welche Antworten bietet sie für die neuen Herausforderungen des Datenschutzrechts? In: Datenschutz und Datensicherheit 40 (9), S. 561-565.

Roßnagel, Alexander/ Geminn, Christian/ Jandt, Silke/ Richter, Philipp (2016): Datenschutzrecht 2016 „Smart“ genug für die Zukunft? Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts. Kassel: Kassel University Press.

Roßnagel, Alexander (2017): Datenschutzaufsicht nach der EU-Datenschutzgrundverordnung. Neue Aufgaben und Befugnisse der Aufsichtsbehörden. DuD-Fachbeiträge. Wiesbaden: Springer.

Rowland, Diane/ Kohl, Uta/ Charlesworth, Andrew (2017): Information Technology Law. Fifth Edition. Routledge.

Sanders, Deen (2014): Reinventing Regulation. In: Law and Financial Markets Review 8 (2), S. 98-102.

Schermer, Bart W./ Custers, Bart/ Hof, Simone van der (2014): The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. In: Ethics and Information Technology 16, S. 171-182.

Sloan, Robert H./ Warner, Richard (2014): Beyond Notice and Choice: Privacy, Norms, and Consent. In: Journal of High Technology Law 14 (2), S. 370-414.

Solove, Daniel J. (2013): Privacy Self-Management and the Consent Dilemma. In: 126 Harvard Law Review, S. 1880-1903.

Stalder, Felix (2011): “Autonomy beyond privacy? A rejoinder to Bennett”, In: Surveillance & Society 8 (4), S. 508-512.

Sztompka, Piotr (1999): Trust. A Sociological Theory. Cambridge: University Press.

Tayler, Linnet/ Floridi, Luciano/ Sloot, Bart van der (2017): Introduction: A New Perspective on Privacy. In: Taylor, Linnet/ Floridi, Luciano/ Sloot, Bart van der (Hg.): Group Privacy. New Challenges of Data Technologies. Springer, S. 1-12.

Tutt, Andrew (2017): An FDA for Algorithms. In: Administrative Law Review 69, S. 83-123.

Türpe, Sven/ Geuter, Jürgen/ Poller, Andreas (2017): Emission statt Transaktion. In: Friedewald, Michael/ Lamla, Jörn/ Roßnagel, Alexander (Hg.): Informationelle Selbstbestimmung im digitalen Wandel. Wiesbaden: Springer, 227-248.

Vedder, Anton/ Naudts, Laurens (2017): Accountability for the use of algorithms in a big data environment. In: International Review of Law, Computers & Technology 31 (2), S. 206-224.

Wachter, Sandra/ Mittelstadt, Brent/ Floridi, Luciano (2017): Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. In: International Data Privacy Law 7 (2), S. 76-99.

Waldman, Ari Ezra (2018): Privacy as Trust. Information Privacy for an Information Age. Cambridge: Cambridge University Press.

Walker, Margaret Urban (2006): Moral Repair. Reconstructing Moral Relations after Wrongdoing. Cambridge: Cambridge University Press.

Will, Matthias Georg (2015): Privacy and Big Data: The Need for a Multi-Stakeholder Approach for Developing Appropriate Privacy Regulation in the Age of Big Data. Discussion Paper No. 2015-03 of the Chair in Economic Ethics, Martin-Luther-University Halle-Wittenberg.

Yeung, Karen (2017): Making sense of the European data protection law tradition. In: Biblel, Leighton Andrews et al. (Hg.): Algorithmic Regulation. The London School of Economics and Political Science. Discussion Paper No: 85, S. 34-45. Online verfügbar unter: https://www.kcl.ac.uk/law/research/centres/telos/assets/DP85-Algorithmic-Regulation-Sep-2017.pdf .

Zaner, Richard M. (1991): The Fiduciary Relationship and the Nature of Professions. In: Edmund D./ Veatch, Robert M./ Langan, John P. (Hg): Ethics, Trust and the Professions. Philosophical and Cultural Aspects. Washington: Georgetown University Press, S. 23-44.

Zarsky, Tal Z. (2017): Incompatible: The GDPR in the Age of Big Data. In: Seton Hall Law Review 47 (4), S. 995-1020.