Dark Sides of Data Transparency: Organized Immaturity After GDPR?

Frederik Schade
Copenhagen Business School, Denmark

Organized immaturity refers to the capacity of widely institutionalized sociotechnical systems to challenge qualities of human enlightenment, autonomy, and self-determination. In the context of surveillance capitalism, where these qualities are continuously put at risk, data transparency is increasingly proposed as a means of restoring human maturity by allowing individuals insight and choice vis-à-vis corporate data processing. In this article, however, I draw on research on General Data Protection Regulation–mandated data transparency practices to argue that transparency—while potentially fostering maturity—itself risks producing new forms of organized immaturity by facilitating user ignorance, manipulation, and loss of control of personal data. Considering data transparency's relative "successes" and "failures" regarding the cultivation of maturity, I outline a set of possible remedies while arguing for a general need to develop more sophisticated ethical appreciations of transparency's complex and potentially problematic implications for organized (im)maturity in the digital age.

Key Words: organized immaturity, transparency, personal data, GDPR, informed consent, surveillance capitalism

As citizens, we are increasingly alerted to the opaque processes through which personal data about us are collected, processed, and leveraged by public- and private-sector organizations for a variety of purposes. These practices of data-driven tracking, profiling, and treatment are carried out in ways often largely outside individual and public understanding or control but may still affect and shape people's lives in numerous unpredictable ways (see Mayer-Schönberger & Cukier, 2013; Pasquale, 2015). Richards and King (2013) have called this the transparency paradox of big data. While extensive data collection and analysis may make society and its actors increasingly visible and legible to those able to leverage data for analysis, the process is itself invisible to those being watched and analyzed, its tools and techniques hidden by physical, legal, and technical barriers by design (Richards & King, 2013).

To the extent that a transparency paradox indeed characterizes data-driven surveillance technologies, it would seem to be at the heart of a more general tendency linked to the diffusion of these technologies, which Scherer and Neesham (2020) term *organized immaturity*—a situation in which individuals increasingly delegate their decision-making activities to automated digital systems and impersonal authorities

Business Ethics Quarterly 33:3 (July 2023), pp. 473–501. DOI:10.1017/beq.2022.30
Published by Cambridge University Press on behalf of the Society for Business Ethics.

they cannot possibly comprehend or control, ultimately problematizing the potential for individual enlightenment, autonomy, and self-determination in the face of societal mass digitalization. Today, however, following such events as the Snowden revelations and the Cambridge Analytica scandal, which indicated some of the potential social and political ramifications of extensive data-driven surveillance and intervention, public skepticism has led to widespread calls for increased transparency in relation to the data practices of public and private organizations.

In Europe, the enactment of a General Data Protection Regulation (GDPR) in 2016 (enforceable since May 2018) can be seen as a direct manifestation of such demands for "data transparency" and individual empowerment in the context of organizational data processing (European Commission, 2016). Especially for private-sector organizations, the legality of most data processing activities—particularly for purposes of consumer profiling and "behavioral advertising"—now requires the free and informed consent of the individuals whose behavior is analyzed as data points. By requiring organizations to enact new forms of data transparency and thereby reinstate the possibility of individual enlightenment, autonomy, and self-determination in this context, GDPR may thus be tentatively understood as a regulatory attempt at *reorganizing individual maturity* within increasingly digitalized societies.

But what is the potential of such data transparency practices as a means of reorganizing individual maturity in the digital age? Whereas Scherer and Neesham (2020) point to regulatory interventions like GDPR as, indeed, a potentially effective way of combating organized immaturity and reinstating individual maturity in the context of digitalization, the goal of this article is to delve further into the complexities and potential "dark sides" (see Trittin-Ulbrich, Scherer, Munro, & Whelan, 2021) of data transparency to problematize the assumption that new organizational transparency practices necessarily foster maturity. On the contrary, as I will argue, under certain conditions, organizational data transparency *itself* comes to produce new forms of organized immaturity, thus deeply problematizing its capacity as a potential countermechanism.

The contribution of this article will be to demonstrate and theorize these possible relations between GDPR-mandated data transparency and its capacity to produce organized maturity and immaturity, respectively. Furthermore, it will be to inquire into the conditions of the relative "successes" and "failures" of GDPR-mandated data transparency as a means of reorganizing maturity in the context of private-sector digitalization and its now "consent-based" forms of data processing. This will allow me to propose a set of possible remedies to ensure the quality of new forms of data transparency in the future. Finally, I argue that the institutionalization of data transparency will require a new and more sophisticated ethical vocabulary to ensure its constitution as a de facto countermechanism rather than simply as an additional cog in the systemic production of immaturity.

The article is structured as follows. First, I introduce Scherer and Neesham's (2020) concept of organized immaturity in the digital age and their argument for GDPR as a potential countermechanism. Second, I give a brief presentation of the GDPR framework itself, its historicity, and its particular concept of data transparency. Third, I

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

move on to show how the idealized concept of transparency reflected by GDPR represents a widely held theoretical assumption of transparency's relation to individual maturity—an assumption, however, that has been increasingly challenged by critical research. Fourth—and on this basis—I draw on a growing body of empirical studies of GDPR-mandated data transparency to demonstrate and theorize how such transparency measures come to produce new forms of immaturity as well as maturity. By distilling the conditions of data transparency's relative "successes" and "failures" with regard to the organization of maturity, I present a model of transparency's two-faced—and, thus, potentially problematic—character in this context. Finally, I discuss some implications and argue for the need to develop more sophisticated ethical appreciations of transparency's complex relations to organized (im)maturity in the digital era.

ORGANIZED IMMATURITY IN THE DIGITAL AGE

To frame the theoretical argument of this article, I start by introducing the recently coined concept of *organized immaturity* along with the phenomenon's particular form under digitalization. First of all, the concept of human *maturity* has a long philosophical history but gained particular importance to thinkers like Kant and to the project of the Enlightenment as such. To Kant (1784), human maturity involves the capability of each individual to lead an intellectually reflexive and autonomous life, to exercise choice and ethical decision-making independently of external forms of authority, and to challenge existing institutions from an enlightened point of view. *Immaturity*, by contrast, is characterized by the absence or lack of development of such capabilities and by the individual's decision-making becoming increasingly subjected to forms of external direction and manipulation. In the latter case, Kant also spoke of the propensity for "self-inflicted" immaturity as the situation in which individuals quite willingly surrender their autonomy in favor of being directed through life by an external power (see also Scherer & Neesham, 2020).

On this background, according to Scherer and Neesham (2020: 4), *organized immaturity*, then, represents a situation in which the widespread institutionalization of particular technological infrastructures and "socio-technical systems cause individuals to delegate their decision-making to impersonal authorities they cannot comprehend or control, pushing them into increasingly 'organized' forms of immaturity." Importantly, to Scherer and Neesham, speaking of a sociotechnical "organization" of immaturity does not necessarily imply or presuppose a central authority. Rather, the identification of organized immaturity as a phenomenon derives from the "overall impression … of an orchestrated process of loosely connected socio-technical developments that together push in the same direction and lead to the erosion of individual autonomy" (5). Thus, with the concept of organized immaturity, the question of *who* exactly is "immature" falls into the background while the key object of study becomes, rather, the wider sociotechnical systems characteristic of society and whether—or to which degree—these systems effect tendencies across the socius that challenge or contradict the ideal of individual maturity.

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

In this sense—and as the authors also noted—tendencies toward organized immaturity are obviously not entirely new but have always haunted human societies in different ways. From the structural "enslavement" or "fixation" of individual subjectivities in premodern and medieval societies to restrictions of individual autonomy through legal, disciplinary, and control mechanisms in modern bureaucratic and capitalist societies, the possibilities for individual autonomy have always been restricted in certain ways under various institutional regimes (Berger & Luckmann, 1991) and constellations of power (Deleuze & Guattari, 2013; Foucault, 2007). However, argue Scherer and Neesham (2020), the advent of the fourth industrial revolution, in which digital and data-driven technologies have consolidated as a driving force for societal development, presents new challenges to the project of the Enlightenment, as it has cultivated new and more sophisticated forms of organized immaturity among individuals and collectives. Examples are potentially manifold, from the capabilities of data-driven technologies and "big data" analytics to guide, influence, and manipulate purchasing and voting behavior to "smart" devices—or entire infrastructures, such as "smart cities"—that continuously make decisions for and manage the lives of the humans whose digitally monitored behavior, in turn, feeds the system with continuous flows of data. According to Zuboff (2015, 2019), a useful way to think of these variegated and complexly integrated and dispersed—as well as highly opaque—sociotechnical infrastructures is as the "Big Other": a technologically mediated network of power connecting a plurality of private and governmental actors. According to Zuboff, this Big Other facilitates both unprecedented forms of data-driven surveillance and control and is geared toward making human behavioral modification the key ingredient to the profitability and consolidation of a new form of "surveillance capitalism" (see also West, 2019).

The crucial point here is that this tendency of commodifying behavioral data and constituting human behavioral modification as a source of profit in capitalist societies seems to directly challenge the ideal of individual maturity (including individual enlightenment, autonomy, and self-determination) described earlier. For example, practitioners of digital behavioral advertising—the initial economic successfulness of which was arguably key to the birth of surveillance capitalism (Zuboff, 2015, 2019)—often pride themselves with a form of paternalism when arguing that new forms of data-driven tracking and profiling allow them to "know you better than you know yourself," including the details of someone's personality traits as well as effective ways of satisfying one's desires in increasingly efficient and proactive ways (see, e.g., Mayer-Schönberger & Cukier, 2013). At the same time, surveillance capitalism appears to entail new incentives for individuals to engage in self-inflicted forms of immaturity, that is, to voluntarily submit to surveillance and direction from an external authority to benefit from the possibilities, conveniences, and forms of security this may entail (consider, e.g., the growing dependence on Google Assistant to guide and facilitate one's daily activities) (see Whelan, 2019, 2021). Furthermore, the inherent technological complexity of these systems—that is, their "black-boxed" character (see Pasquale, 2015)—makes contemporary surveillance technologies deeply opaque and unintelligible to the people whose

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

behavior is datafied, scrutinized, and manipulated to ensure higher levels of profit and control (hence the aforementioned transparency paradox). At a fundamental level, this built-in opacity seems in itself to challenge the cultivation of individual maturity in the digital era insofar as general unawareness of the ubiquity and functionality of these systems disables the possibility of individual and public enlightenment, reflexivity, and, ultimately, political deliberation in relation to the purpose of new surveillance infrastructures.

Noting how technological and systemic opacity as well as the lack of individual and public awareness of this emerging sociotechnical regime indeed comes to constitute a key issue for Scherer and Neesham's (2020) diagnosis of organized immaturity, it might seem unsurprising that regulatory *transparency* is proposed as a solution to the issue of individual enlightenment, autonomy, and self-determination in the digital era. For example, as they write,

> while the explicit narrative [concerning new surveillance technologies] is all positive and imbued with an air of objective inevitability, key decisions about how these systems are being used by a few to extract economic rents and to control the many are not transparent, not democratically arrived at, and not sufficiently regulated by law (4).

On this basis—and while arguing for the specific potentials of a range of societal actors, such as media, businesses, public organizations, and nongovernmental organizations, in combating organized immaturity in the context of digitalization—Scherer and Neesham point to the potential role of the state in "developing legal regulations, procedures and institutions that effectively protect individuals from surveillance and manipulation by the socio-technical complex" (24). In the same breath, and as an example of such lawmaking, they refer explicitly to Europe's new GDPR, enforceable since May 2018, and its "informed consent"–based provisions as an example of one such potentially effective way of counteracting organized immaturity and cultivating individual enlightenment, autonomy, and self-determination in the digital age.

As mentioned, the aim of this article is to discuss the potential of GDPR in this regard and its transparency provisions, including its notion of "informed consent" as an effective remedy to counteract organized immaturity and reorganize individual maturity in the context of private-sector digitalization. To do so, I start by giving a brief introduction of GDPR, its concept of transparency, and how it relates to the question of individual maturity.

THE EUROPEAN REGULATORY SOLUTION

To understand how GDPR relates to the question of individual maturity in the context of digitalization and its new forms of data-driven surveillance and interventionism, it is worth noting how the legal framework defines the problem according to the concept of "privacy." This idea of a legal right to privacy dates back to the late nineteenth century and the conception of a "right to be let alone" (e.g., free from external surveillance and/or manipulation) that, according to Brandeis and Warren (1890), could be established under US common law. In a European context, the idea

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

of an individual right to privacy only gained real traction after the atrocities committed against the Jews during World War II, as, for example, the creation of the Jewish Registry from national census data allowed the Nazis to locate many of their Jewish victims. After the war, such events led to initial formulations of a legal right to privacy, first by the United Nations in the Universal Declaration of Human Rights in 1948 and later in the European Convention on Human Rights in 1950. However, it was not until the adoption of the European Charter of Fundamental Rights in 2009 that the protection of such rights became legally binding for European Union (EU) member states to enforce. Specifically, Article 8 of the charter provides that everyone has the right to the protection of personal data; that such data must be processed fairly, for specific purposes, based on individual consent or another legitimate basis; and that the individual has the right to access data concerning him or her and to have it rectified. Finally, it provides that these rules shall be subject to control by an independent national authority (for an overview, see Trzaskowski & Sørensen, 2019).

The basic principles of the charter were further elaborated in the EU Data Protection Directive, which was adopted in 1995. However, as a "directive," its legislative effectiveness largely depended on individual member states' willingness to implement its rules into national legislation. Thus, in 2011, the EU recognized the need for an altogether stronger and unified regulation that would be directly applicable in all member states. Finally, after its formal adoption in 2016, this GDPR effectively replaced the preexisting directive in May 2018 (European Commission, 2016). Since then, GDPR has been widely celebrated as a hallmark regulation for strengthening the fundamental rights to privacy and data protection of individuals in the digital age as well as clarifying and harmonizing the rules for businesses and other organizations in the digital single market. Importantly, GDPR does not regulate practices of personal data processing only within the European territory but regulates the processing of data relating to EU citizens *wherever* such processing occurs. Hereby, GDPR effectively constitutes a piece of extraterritorial (even global) regulation, as its rules apply to organizations anywhere that process data on EU citizens (see, e.g., Goldsmith & Wu, 2006).

Extending the provisions of the EU charter and the preexisting directive in several respects, GDPR lays forth an elaborate framework of principles (e.g., purpose limitation, data minimization, fairness, transparency, accountability), legitimate bases for data processing (e.g., individual consent, contractual relationships, legal obligations, legitimate interests), and general practical obligations according to which organizational data processing must be conducted. The framework further specifies a set of data subject rights (e.g., a right to information; of access; of rectification, erasure, and restriction; to data portability; to object; and to an explanation in certain cases where one is subjected to decisions based on automated processing), along with a set of provisions defining appropriate enforcement mechanisms at both the EU and national levels (Goldsmith & Wu, 2006).

A more elaborate presentation of GDPR's general framework, however, is beyond the scope of this article. Instead, I turn to focus specifically on the regulation's concept of transparency and its relation to the notion of "informed consent" that provides the

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

most common legal basis for private-sector personal data processing. Importantly, while this article focuses specifically on GDPR's transparency obligation as a potential countermechanism to organized immaturity, one could rightly argue that GDPR as such (and not just its transparency requirements) might be conceived as a means of counteracting organized immaturity under digitalization. For example, in certain cases, GDPR has already proven to be an effective legal framework for protecting individual rights to privacy by holding big tech firms like Google and Facebook accountable.[1] In this article, however, by focusing on GDPR-mandated transparency measures in particular—for example, in the form of organizational privacy policies, website cookie notices, and consent mechanisms with which most Europeans will be familiar—I draw attention specifically to concrete instances in which the individual might (based on existing regulation) exercise a right to privacy in his or her everyday life. I do so arguing that these everyday decision-making practices by individuals to give or withdraw consent to data-driven tracking now represent an important site for the potential cultivation of maturity and/or immaturity in the digital era. Hereby, I also limit myself from considering individuals' "right to an explanation" in certain particular cases of algorithmic decision-making where decisions are legal or otherwise "serious" in nature, although this mechanism might be seen as an important form of "data transparency" after GDPR. Finally, I limit myself to considering data processing in the private sector, because the rules for public-sector data processing are different in kind and constitute a separate and complex matter beyond the scope of this article.[2]

Thus, following the regulation's enactment, the lawfulness of data processing in most cases in which private companies process personal data on nonemployee individuals—for example, existing or potential customers in the case of data-driven behavioral advertising—depends entirely on those individuals' (i.e., data subjects') "informed consent." Such consent is further defined as "any freely given, specific, informed, and unambiguous indication of the data subject's wishes" with regard to organizational data processing (see Article 2[11]). Thus, in relation to the sociotechnical complex of surveillance capitalism described earlier, the requirement of informed consent to data processing constitutes a safeguard to the preservation of individual privacy and autonomy in the context of private-sector data accumulation. It guarantees, in other words, one's freedom from such data processing until one gives explicit and informed consent. This also means that the individual retains, in principle, a right to refuse any such otherwise "unnecessary" processing of personal data, that is, processing that is not

[1] For example, in 2020, the Court of Justice of the European Union sided with lawyer and activist Max Schrems by invalidating the existing legal basis for personal data transfers from the European Union to the United States (the European Commission's "Privacy Shield Decision"), stating that data transfers had to meet stricter requirements to comply with GDPR (European Parliament, 2020).

[2] For example, generally speaking, most public-sector processing is not consent based but usually "necessitated" by the legal obligations of particular public bodies and the state as such (see European Commission, 2016).

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

necessitated by some alternative legal basis, such as contractual relationships with or other legal obligations of the particular company.

According to GDPR, this decision by the individual to give or withdraw consent to organizational data processing has to be "informed," which is the point where transparency becomes relevant. According to the Working Party Guideline on the subject, transparency constitutes an "overarching obligation" within the GDPR framework and concerns the provision of information from "data controllers" (the organization determining the purposes and means of data processing) to "data subjects" (natural persons to whom those data relate). Introducing the concept and purpose of transparency as intended by the regulation, it states,

> Transparency is a long-established feature of the law of the EU. It is about engendering trust in the processes which affect the citizen by enabling them to understand, and, if necessary, challenge those processes. . . . Transparency, when adhered to by data controllers, empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent and actioning their data subject rights (Article 29 Working Party Guideline, 2018: 5–6).

It is through definitions like this one that we start to get a sense of the key role of transparency as imagined in relation to the cultivation of individual maturity in the digital age. First of all, following the regulation and its principles, it is clear that the quality of data subjects' decision whether to consent to processing essentially depends on organizations' ability to 1) keep individuals informed of the existence, nature, and scope of data processing and 2) allow individuals to exercise their rights, including the right to control these processing activities by providing or withdrawing informed consent. Thus the entirety of this interaction—or transaction—between the organization (data controller) and the individual (data subject) must be "transparent" to individuals, and this "transparency" should be assured by the organization seeking to collect and process personal data. Second, this envisioned transparency is presented as an effective means of reducing (or even neutralizing) imbalances of power between organizations and the individuals from whom they seek to gather personal data. This should be achieved as individuals become (fully) informed about the occurrence and nature of organizational data processing and—based on this enlightenment—able to both challenge but also more generally to exercise complete control over these processes in a free and reflexive manner. Third, and ultimately, transparency is meant to cultivate a relationship of trust between the parties involved. One may note that in this idealized situation, "trust" becomes seen as intimately tied to—or, more precisely, dependent on—the cultivation of individual maturity as it presumes not simply a passive but an *active* and enlightened acceptance of organizational data processing based on a comprehensive understanding of and ability to reflexively control those processes by the individual.

We thus arrive at the key tenets of an ideal scenario in which GDPR is presented as a means of effectively countering organized immaturity and reinstituting individual maturity in the digital age by cultivating individual enlightenment, autonomy, and reflexive self-determination in the context of private data processing. As we shall see

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

in the following section, this idealized theory of transparency as a means of cultivating individual maturity is already common to the established literature on organizational transparency. However, such idealized conceptions of transparency have also been increasingly problematized by a number of critical contributions that, in different ways, all point to the problems and potential paradoxes associated with organizational "transparency."

TRANSPARENCY: FROM ENLIGHTENMENT TO PARADOX

The idea of organizational transparency as a means of enlightenment, empowerment, and thus to the cultivation of individual maturity is widely present in existing literature. Transparency is commonly understood as a way of making organizations and their practices visible to their publics, providing individuals with a level of insight and control vis-à-vis the institutions that affect their lives (Hood & Heald, 2006). Thus theorized, transparency is largely equated with organizations' publication of information about their practices, where such information provision—for example, concerning practices of data collection, processing, and circulation—is supposed to ensure accountability and advance democratic practices and values (Fung, 2013; Garsten & de Montoya, 2008). Organizations are, in other words, expected to respond to societal demands by acting as open and benevolent providers of information so that individual citizens and other actors may gain knowledge about existing practices and hold organizations accountable (Erkkilä, 2012; Rawlins, 2009). Ultimately—and just as envisioned by legal frameworks like GDPR—transparency is assumed to install relations of trust between organizations and their stakeholders, where such "trust" presumes both individual enlightenment and empowerment (e.g., Best, 2007; Schackenberg & Tomlinson, 2016). This common view, I argue, seems to imply a necessarily positive relationship between transparency and the cultivation of individual maturity—an assumption that is made somehow explicit by Rawlins (2009: 75), who sees organizational transparency as a way of "enhancing the reasoning ability of publics and holding organizations accountable for their actions, policies, and practices."

This common conception of transparency has, however, been increasingly challenged by a growing stream of critical research for not considering the inherent tensions, problems, and paradoxes associated with organizational transparency (e.g., Christensen & Cheney, 2015; Christensen & Cornelissen, 2015; Fenster, 2006, 2015; Roberts, 2009, 2018; Strathern, 2000). For example, transparency—it is argued—constitutes an inherently political phenomenon, involving a set of complex negotiations about what transparency should and should not render visible (Albu, 2014; Fung, Graham, & Weil, 2007; Heald, 2006; Thedvall, 2008). Such inherent limitations are also associated with the kind of technical medium used to produce transparency, as the specific affordances of this medium necessarily shape and limit any possibility of insight (Hansen & Flyverbom, 2015). As Albu and Flyverbom (2019) point out, concrete transparency practices, thus, always facilitate specific ways of knowing, which, in turn, always produce new types, forms, or levels of opacity (see also Flyverbom, 2019; Ringel, 2019). This occurs when organizations

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

selectively disclose information to their own advantage (e.g., Heil & Robertson, 1991; Heimstädt, 2017), rely on ambiguous statements to manage potential issues (Eisenberg, 2007), use information disclosures to limit potential liabilities (O'Neill, 2006), or develop policies merely to stay formally compliant with external demands and deflect critical stakeholder attention (see, e.g., Meyer & Rowan, 1977). Even in situations where information disclosures are used as deliberate attempts to limit potential insight, the amount, density, and complexity of information may overwhelm intended receivers, effectively deterring further scrutiny (Stohl, Stohl, & Leonardi, 2016). The assumed capacity of transparency to restore public trust seems equally problematic when considering instances in which practices of accountability and openness instead lead to increased distrust in organizations and institutions (O'Neill, 2002). These critical perspectives on the limitations and paradoxes associated with organizational transparency are generally concerned with transparency's inherent *performativity* (MacKenzie, 2006), that is, the fact that transparency may "do things" and affect both organizational practices and audiences in a number of unintended ways (see also Albu & Flyverbom, 2019; Roberts, 2009).

Inspired by this general performative view of organizational transparency, the next section delves into the potential limitations and complexities surrounding particularly GDPR-mandated data transparency and its (in)capacities as a potential countermechanism to organized immaturity in the digital era. Doing so, I seek to illustrate and theorize how new forms of data transparency intended to serve as an effective means of cultivating individual maturity may—under certain conditions—come to serve as just an additional cog in the sociotechnical apparatus for organizing immaturity identified by Scherer and Neesham (2020) (see earlier). This illustration further allows me to distill the conditions of the relative "successes" and "failures" of data transparency in relation to the cultivation of maturity, on which basis it becomes possible to suggest potential remedies and strengthen data transparency's potential as a countermechanism to organized immaturity.

DATA TRANSPARENCY AND (IM)MATURITY

According to GDPR, the required information that, in general, data controllers should provide to data subjects constitutes a long list of "facts," including the identity and contact details of the responsible party, the purposes and legal basis for processing personal data, categories of data concerned, recipients or (importantly) categories of recipients of those data, information on transfers to third countries, the storage period, the data subject's rights, the source of data (if not acquired directly from the data subject), and information on automated decision-making, if applicable (European Commission, 2016). This list of information requirements largely defines GDPR's obligation of transparency, that is, the predefined set of facts data controllers must provide data subjects to comply with existing regulation. Furthermore, because GDPR (in most cases, as explained earlier) requires that companies acquire the data subject's informed consent before processing personal data relating to the subject, the most common way to practically enact transparency for a given company is through a publicized privacy policy as

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

well as various "notice and consent" mechanisms on its company website (so-called cookie banners). It is typically through the latter mechanism that individual data subjects may provide or withdraw consent through an interactive interface (Nouwens, Liccardi, Veale, Karger, & Kagal, 2020), thus exercising their right to privacy under existing regulation.

To ascertain how such GDPR-mandated transparency practices relate to organized immaturity in the context of private-sector digitalization, the key question will be to which degree new transparency practices actually enable individual enlightenment, autonomy, and self-determination in this context. As I show, however, not only is GDPR-mandated transparency's potential limited in this regard but transparency itself risks becoming directly counterproductive to the ideal of maturity as it produces new forms of organized immaturity among individuals. I argue, this happens specifically when transparency itself becomes a means for the systemic production of *ignorance*, *manipulation*, and *control loss* among individuals—notions which, in the following, I develop as a set of conceptual categories to better enable us to recognize the dark sides of data transparency.

Enlightenment versus Ignorance

Considering the findings of existing research on post-GDPR transparency practices, most studies have found GDPR to have indeed led to increased information disclosures among organizations (see Degeling, Utz, Lentzsch, Hosseini, Schaub, & Holz, 2019; Linden, Khandelwal, Harkous, & Fawaz, 2020; Sanchez-Rola et al., 2019; Utz, Degeling, Fahl, Schaub, & Holz, 2019). For example, Degeling et al. (2019) found that 84.5 percent of the most popular websites in the EU had published privacy policies after May 25, 2018, when GDPR took effect, and that 72.6 percent of them updated their policies close to this date. Regarding the quality of such policies, another study by Urban, Tatang, Degeling, Holz, and Pohlmann (2018: 11) of companies that shared personal data with third parties found that 36 of 39 (92 percent) "[fulfilled] the minimum requirements for privacy policies" imposed by the law. Additionally, some studies, such as Linden et al. (2020), have found company privacy policies after GDPR to be generally more attractive and clearer, longer, and more comprehensive, covering a larger number of relevant topics (such as data retention, handling of special audiences, and user access), as well as more specific in their coverage, than pre-GDPR policies.

Whereas such a tendency toward increased information disclosures by companies could be seen to enable new levels of transparency in the context of private data processing, it is also initially worth noting how a number of studies point to significant variation in the quality of the information disclosed (see, e.g., Linden et al., 2020; Mohan, Wasserman, & Chidambaram, 2019; Tesfay, Hofmann, Nakamura, Kiyomoto, & Serna, 2018). First of all, while suggesting a trend toward increased regulatory compliance in company disclosures, the preceding numbers also suggest that not all company websites studied included a privacy policy in the wake of GDPR. Urban et al. (2018: 20) further described how "not all companies take their legal obligations seriously" as, in some cases, existing policies seemed to be missing legally required information. In a different study reviewing the landscape

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

of organizational cookie notices after GDPR, Utz et al. (2019: 4) noted that "[while] nearly all notices (92%) contain a link to a privacy policy, only a third (39%) mention the specific purpose of the data collection or who can access the data (21%)." Furthermore, considering how companies describe the purposes of data collection, they noted that such descriptions were either "specific (e.g., 'audience measurement' or 'ad delivery'; 38%), generic (e.g., 'to improve user experience'; 45%), or not specified at all (16,9%)" (4). While on one hand implying possible forms of best practice in the way organizations formulate their information disclosures, such variation in informational quality, on the other hand, also points to ways in which transparency's potential for cultivating the enlightenment of individuals (i.e., data subjects) in the context of data processing may become limited by organizations' pursuit of their own agendas or by simple negligence.

However, if we turn to consider the situation from the perspective of the individual data subject, the supposed positive relationship between GDPR-mandated transparency measures and individual enlightenment becomes altogether more problematic. As several studies have noted, organizational privacy policies are notorious for taking a disproportionate amount of time for individuals to acquaint themselves with and often require reading comprehension abilities at university level (see, e.g., Jensen & Potts, 2004; McDonald & Cranor, 2008). As a result, website users hardly ever read website privacy policies (Nissenbaum, 2011; Obar & Oeldorf-Hirsch, 2018) and have been shown to often "automatically" consent without viewing them (Angulo, Fischer-Hübner, Wästlund, & Pulls, 2012; McDonald & Cranor, 2008). Studies suggest that this behavior—which might initially appear as a kind of "self-inflicted" immaturity (see earlier)—often results from the experience of individual data subjects of "consent fatigue" and that such policies and cookie banners simply "stand in the way" of their primary goal: accessing a given website (Acquisti & Grossklags, 2005; Nouwens et al., 2020). Thus such behaviors, which might appear as self-inflicted immaturity in this context, could just as well be argued to result from what is sometimes referred to as information overload, that is, the deliberate and systemic overburdening of individuals with large amounts of information. For example, McDonald and Cranor (2008) have shown how reading all privacy policies the average individual encountered on an everyday basis, he or she would need approximately 244 hours per year to do so.

Initially, we might say that such contextual inappropriateness in the way information is provided by organizations to data subjects provides another rather sharp limit to the degree of enlightenment one might expect new forms of data transparency to accomplish. But this, however, would itself be a limited view. Rather, because the resulting situation becomes one in which 1) the data subject may have to make a consent decision before visiting a website but 2) cannot possibly acquaint himself or herself with all the information relevant to that decision, data transparency suddenly becomes productive of a particular form of ignorance rather than enlightenment. This to the extent that "information overload" and the use of selective and/or ambiguous language in organizational privacy policies in practice forces the individual data subject to make consent decisions without being able to understand the full set of terms relevant to that decision. In other words, whether or not the

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

individual decides to consent to organizational data processing, the individual will likely not have understood exactly that to which he or she was consenting or from which he or she was withdrawing consent.

The key issue here seems to amount to a question of the *contextual legibility of terms*, that is, whether the individual in a given situation can reasonably process the terms of a consent decision. In situations where consent decisions come to be made based on terms the individual *cannot* reasonably comprehend and process (which seems common in the context of data processing), data transparency itself becomes a means of fostering ignorance rather than enlightenment in cases where the individual leaves the transaction unaware of that to which he or she may have consented.

Autonomy versus Manipulation

Of course—one might argue—the individual remains free to decide *not* to consent to forms of data processing that he or she does not fully comprehend. At this point, we are moving toward the question of transparency's ability to cultivate individual autonomy, understood broadly here as the freedom of choice regarding whether to give consent to data processing. As described earlier, GDPR remains clear that the consent of individuals to data processing should not only be "informed" but also "freely" given (European Commission, 2016). With regard to the practices and technologies organizations use to facilitate individual data subjects' consent decisions (i.e., interactive cookie banners or interfaces), this is usually taken to mean that the individual should be presented with a clear choice, where it must be "as easy to withdraw as to give consent [to data processing]" (European Commission, 2016; see also Court of Justice of the European Union, 2019). This is meant to enable the individual data subject the kind of free and uncoerced decision-making envisioned by GDPR's transparency provision (see earlier).

According to several studies, however, the extent to which GDPR-mandated transparency measures in practice allow for such autonomous decision-making by individuals is highly questionable. These studies all point out ways in which many companies actively seek to make it harder for individuals to exercise their rights under GDPR. Particular attention has been paid to the use of "dark patterns" in the design of website consent interfaces. For example, in a study of consent interfaces among 680 top UK websites, Nouwens et al. (2020) showed how 1) the vast majority made rejecting all tracking substantially more difficult than accepting it (i.e., only 12.6 percent of websites displayed a "reject all" function with the same or fewer number of clicks than the "accept all" function); 2) one-third of the websites relied on "implicit consent," where a number of alternate actions the individual takes on the website are taken to "count as" the individual giving consent to tracking; and 3) widespread use of preticked boxes (each representing different purposes of data processing) in cookie interfaces so that individual data subjects have to actively click through and detick each individual box to effectively reject tracking. Such usage of "dark patterns" in the design of consent interfaces—all in different ways geared toward forcing or "nudging" individual data subjects to consent to tracking—are considered illegal under GDPR (Nouwens et al., 2020; see also Court of Justice of the European Union, 2019), yet their use is ubiquitous among the majority of

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

websites within and beyond the EU that process data on its citizens. Altogether, only 11.8 percent of the consent interfaces Nouwens et al. (2020) studied were found to be fully compliant with GDPR's design prescriptions.

And as the authors went on to show, the choice of design pattern may significantly influence individual decision-making. For example, removing the immediately visible "reject all" function increased the probability of consent by at least 22–23 percent (Nouwens et al., 2020). Hereby, exactly those concrete mechanisms of data transparency that were meant to enable autonomous decision-making by individuals may themselves be—and, in this context at the time of writing, *tend to be*—designed by companies to limit that same autonomy and introduce various forms of manipulation into the situation of individuals' consent decisions. Thus the mechanism of "transparency" supposed to work as a safeguard of individual autonomy in the context of surveillance capitalism is itself turned into an additional means of manipulation aimed at constricting that same autonomy in turn.

The problem seems to lead to a question of *choice equality*, that is, whether data transparency offers the individual an equal choice between consenting to or refusing tracking. This would contrast situations in which choice options become unequal or entirely absent, whereby data transparency progressively turns into a means of manipulation rather than of enabling individual autonomy. A crucial detail in this regard seems to be that the absence of an explicit decision by the individual should always be regarded as a refusal of tracking, because consent—according to GDPR—must be explicit (as noted earlier). Organizations' reliance on "implicit consent" as a legitimate basis for data processing could thus be argued to amount to the denial of a meaningful and equal choice with regard to data processing and thus a denial of autonomy.

Self-Determination versus Loss of Control

Now, suppose that some individual takes his or her privacy quite seriously and on a daily basis actively does everything he or she can to carefully manage these consent decisions to stay in full control of personal data sharing. The question becomes whether and to which degree GDPR-mandated transparency mechanisms actually enable such individual self-determination, understood broadly as the possibility of retaining and administering control over one's data. Here not just the design but also the functionality of website consent interfaces becomes relevant. To which extent do active decisions by the individual to consent to or reject tracking actually enable individuals to stay in control of their data? Do the technical mechanisms work as they are supposed to?

Only a few studies have considered this matter. The few that have, however, paint a troubling picture. An example of such a study by Sanchez-Rola et al. (2019) considered the impact of GDPR on cookie-based tracking and user consent among websites that should be affected by the regulation. Starting from the conception of GDPR as an extraterritorial regulation applying to any company that processes personal data on EU citizens, they investigated the functionality of two thousand websites hosted both within and beyond the EU. Initially, they found GDPR to have impacted website behavior in a truly global way, as, for example, US-based

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

websites appeared to implement cookie regulations in a similar fashion to EU websites in terms of information disclosures and opt-out options. At the same time, however, they could document how tracking of EU citizens on websites internationally was still prevalent, was ubiquitous, and happened mostly without user consent. By visiting each website and choosing "opt out" whenever possible, they sought to measure the relative ease and efficiency of rejecting tracking. According to their findings, most websites performed some form of tracking, and a remarkable 92 percent did so already *before* providing any notice to the user. At the time, only 4 percent of these websites provided a clear opt-out option in their cookie interfaces, and even when they did, the choice to opt out was often technically ineffective. That is, in most cases, the number of cookies the server set remained stable or even *increased.* Altogether, the cases in which at least *some* cookies were erased after rejecting them were, on average, only 2.5 percent of the entire population of websites. These findings led the authors to conclude that the most visible effect of GDPR among company websites was an increase in available information on the legitimacy of tracking practices rather than any significant changes to those practices themselves—even when users actively choose to opt out.

Another study, by Urban et al. (2018), described a similar situation resulting not from deficient technical functionalities but from a potential "gap" in the formulation of the GDPR regulatory framework itself. This study was concerned specifically with the state of the digital advertising "ecosystem" (i.e., the kind of data-sharing networks Zuboff described as the "Big Other," through which personal data are traded and distributed instantly, in real time, among multitudes of companies) after GDPR took effect. On one hand, they found that almost all the companies investigated (36 out of 39) had disclosed privacy policies that all fulfilled the minimum requirements of GDPR. On the other hand, however, they found that as company websites shared tracking data with third parties, the complexity of the digital data-sharing networks among companies worked in such a way that embedding a single third party into a website put individual users at risk that their data would get shared with hundreds of other companies. As noted, GDPR only requires companies to inform individuals of the "categories of partners" with whom they share data, not the specific parties. As the authors note, this situation "leads to the problem that users cannot verify who has received a copy of information about them and leads to the question how service providers can ensure that data is deleted upon request" (11). In this case, we see how the particular legal requirements imposed on companies by GDPR do not necessarily support or ensure the ideal of individual self-determination envisioned by the regulation's transparency provisions (see earlier). As the authors note, "in this case, the users have virtually no chance to keep control over their data" (20). As personal data are shared instantly among companies and third parties—for example, through "real-time bidding"—each with its own sharing connections, potential breaches, and so on, it becomes virtually impossible for anyone (including individual data subjects but also individual companies themselves) to keep track of the complex networks through which personal data circulate and thus to meaningfully guarantee the right of the data subject to retain control of those data. In both cases—dysfunctional opt-out mechanisms and apparent regulatory "gaps" in the

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

GDPR framework itself—what is interesting is that the particular way organizations come to enact data transparency in practice makes it effectively impossible (rather than possible) for the individual to maintain control of his or her data. Thus the advent of data transparency not only signals increasing amounts of data control by individuals but also the opposite, that is, new ways for individuals to effectively be denied control of data related to their persons.

The key problem here seems to be one of *choice efficiency*, that is, whether data processing or sharing occurs *beyond* that to which the individual has actively consented, that is, whether one's choice to consent is practically efficient in relation to data one is legally entitled to control. When it is not, data transparency itself—rather than constituting a means of ensuring individual self-determination—effectively produces new forms of control loss among individuals.

Implications for Organized (Im)maturity

To sum up, GDPR-mandated transparency might, on one hand, be said to cultivate—or hold the potential to cultivate—individual maturity in relation to private-sector digitalization, this to the extent that increased levels of mandatory information provision in fact enable individual enlightenment, as well as situations in which new consent technologies in fact sustain individual autonomy and self-determination in relation to private data processing. On the other hand, it should be clear from the preceding discussion that GDPR-mandated data transparency—depending on the specific way organizations enact it—may in many ways have come to serve as yet an additional cog in an existing technological complex geared toward organized immaturity, this to the extent that data transparency mechanisms become mobilized as means for organizations to produce ignorance, manipulation, and loss (rather than the insurance) of control of personal data among individuals. What is remarkable is that GDPR-mandated data transparency in this case comes to coproduce the exact problem it was originally meant to resolve. Furthermore, whereas GDPR-mandated data transparency arguably does hold a potential to ensure and sustain individual maturity, the tendency emerging from existing research is, rather, indicative of the systemic production of ignorance in the context of individual consent decisions (i.e., the "automatic" provision of consent), of elaborate and widespread uses of manipulative design patterns in the making of website cookie interfaces, and of dysfunctional technical solutions and regulatory loopholes that effectively make it impossible for even the most privacy-concerned individuals to retain control of their personal data. In this situation, data transparency ultimately comes to produce new forms of organized immaturity rather than counteracting it.

To restore transparency's potential as a means of cultivating individual maturity rather than of further organizing immaturity, the foregoing analysis has allowed for the distillation of a set of variables that appear to determine the relative "successes" and "failures" of data transparency in this regard. I have attempted to illustrate this conditionality of data transparency's potential to reorganize individual maturity versus further contributing to the production of organized immaturity in the model of Figure 1.

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

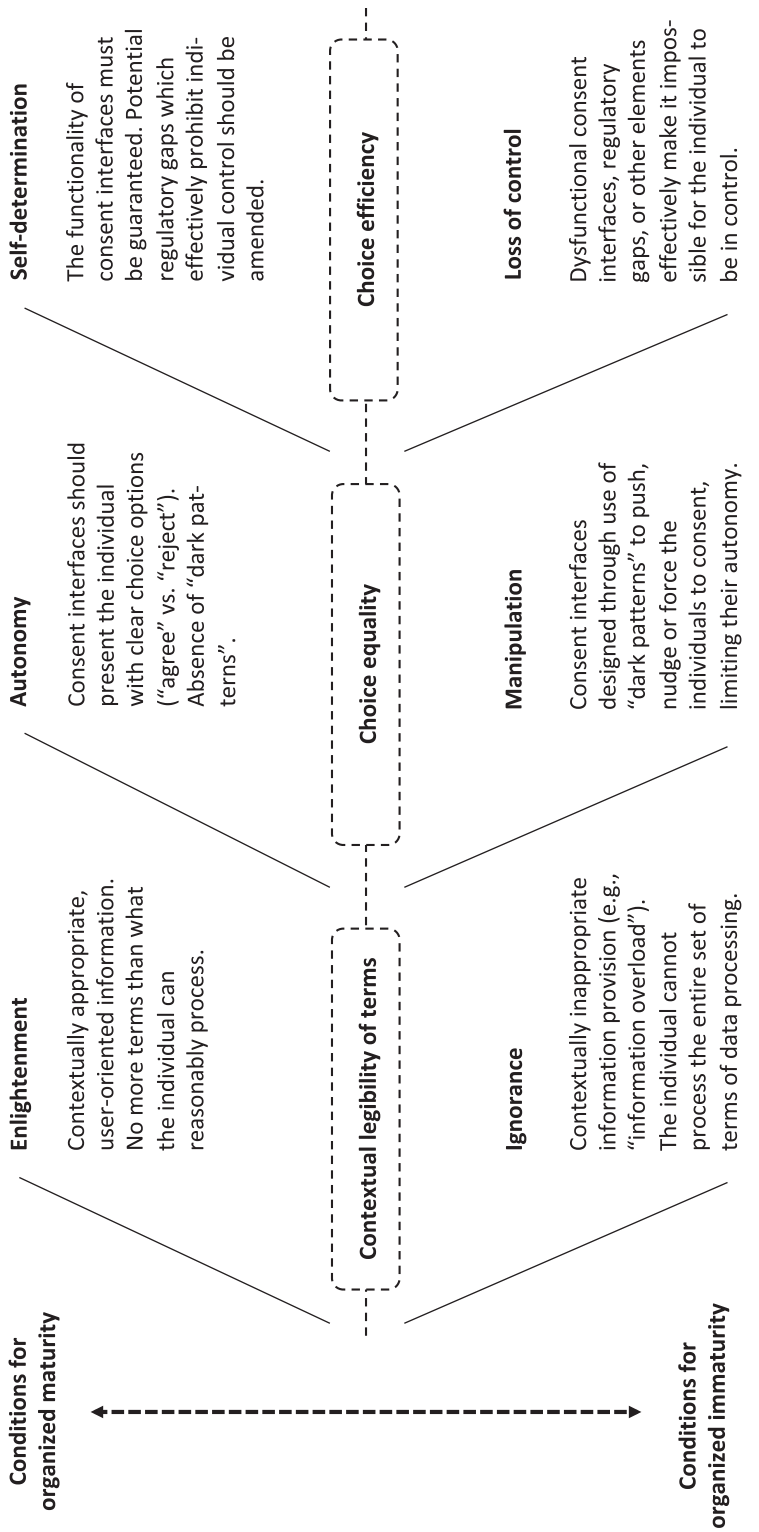

Figure 1: Data Transparency as a Source of Organized Maturity and Immaturity

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

Importantly, although this article does not engage in measuring these variables, it suggests that a higher degree of each variable pushes data transparency's potential toward the production of maturity, while a lower degree pushes this potential toward the production of immaturity. Thus, as the model illustrates, GDPR-mandated data transparency might hold a potential to function as an effective countermechanism for organized immaturity in the digital age. However, the realization of this potential will require several adaptations to the way organizations tend to enact data transparency in the existing digital environment and may even require certain particular adjustments to GDPR's legal framework itself.

First, a key variable to determine whether transparency fosters enlightenment or produces new forms of ignorance concerns the *contextual legibility of relevant terms.* Here information disclosures meant to ensure the enlightenment of data subjects should be user oriented and comprise no more information or terms than the individual can reasonably process. The moment information disclosures become too complex and comprehensive for the individual to process in the given situation (e.g., quickly, as he or she enters a website), the production of ignorance is inevitable, as the individual will be making consent decisions based on terms he or she cannot reasonably read and understand and of which he or she may be entirely unaware. This perspective might have the further consequence that organizations—in the name of transparency—may have to refrain from using data for a great variety of complex purposes and should gather data instead for single, specific purposes only.

The second variable indicates transparency's ability to foster individual autonomy versus entailing new forms of manipulation and concerns the *equality of choice.* Here website cookie interfaces should always present the individual with an equal choice between accepting and rejecting tracking. No variety or form of manipulatory "dark pattern" design can be regarded as acceptable if the objective is to ensure and sustain individuals' autonomous decision-making. Furthermore, and as argued earlier, organizational reliance on "implicit consent" as a legitimate basis for personal data processing might be understood as a denial of autonomy (in the sense of a free and equal choice) and should therefore be considered illegitimate.

Finally, the third variable of *choice efficiency* designates data transparency's ability to ensure individual self-determination versus causing new forms of control loss among individuals. Here any aspect of the interaction between data subjects and data controllers that prohibits the efficiency of the data subject's decision-making (whether technical dysfunctionality, regulatory loopholes, etc.) should be amended to ensure that it is indeed feasible for the data subject to retain control of personal data. As long as it is not, data transparency cannot be considered an effective means of ensuring individual self-determination, constituting instead merely a new mechanism of denying individuals control of their data.

If such adaptations are made, the potential of GDPR-mandated transparency measures to recultivate individual maturity in the context of contemporary surveillance capitalism is likely to increase significantly. This would be from the current situation, however, in which data transparency most unfortunately tends to produce new forms of organized immaturity rather than acting as an effective safeguard against the phenomenon.

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

DISCUSSION

In this discussion, I wish to accomplish three things. First, I discuss possible additional complexities characterizing the relationship between data transparency and the organization of (im)maturity in the context of digitalization. This involves inquiring into the "bigger picture" of the current situation and question whether and to which degree measures like GDPR-mandated data transparency will ever be capable of reorganizing maturity in this context. Raising this question, however, enables me to propose possible avenues for future research. Second, I argue for why organized immaturity constitutes a threat worth acting upon in the context of surveillance capitalism relative to other domains of modernity, where the risk may be less substantial. Third, with a mind toward practitioners in the area of post-GDPR data protection, I discuss and argue for the need to develop more sophisticated ethical appreciations of transparency's complex—and, as we have seen, potentially problematic—relationship with organized (im)maturity. This should allow us to better apprehend and address the limits and counterproductive effects of data transparency in the future.

To understand the complex relations between data transparency and the organization of (im)maturity, an important question is whether data transparency is always or necessarily supposed to cultivate maturity at all or whether it might have alternate purposes as well. To explore this question, let me start by considering an important aspect of the existing situation I have yet to touch upon, namely, the question of legal enforcement. The question of enforcement seems immediately relevant when noting—as I have done previously—several existing challenges resulting from relatively high levels of organizational noncompliance with GDPR and its transparency requirements. This includes—as we have seen—significant variations in the quality of information disclosures, widespread use of manipulative "dark patterns" in consent interface design, and dysfunctional websites and interfaces that fail to block cookies before or until consent is given. As I have argued, such instances of potentially illegal behavior not only *limit* the capacity of data transparency to foster individual maturity in the context of organizational data processing; as I have argued, they put data transparency at risk of becoming effectively *counterproductive* in this regard insofar as transparency itself comes to produce new forms of ignorance, manipulation, and control loss with regard to personal data among individuals. However, because we are mostly talking about widespread cases of apparent organizational noncompliance, effective legal enforcement could seem like an obvious place to start to address this general problem.

With regard to the question of effective legal enforcement—including the mere threat of sanctions in cases of noncompliance—several recent reports have documented how the capabilities of national data protection agencies (DPAs) charged with enforcing GDPR across EU member states have, since 2018, been impeded by tight budgets, administrative hurdles, and an apparent unwillingness among specific DPAs to enforce existing rules in a sufficient manner (this has been documented particularly in Ireland, where several big tech firms have their European bases of operation; see, e.g., Access Now, 2020; Irish Council for Civil Liberties, 2021). For

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

example, in 2020, the nonprofit organization Access Now could document a total number of a mere 231 fines and sanctions levied by national DPAs between May 2018 and May 2020—a seemingly low number compared with the total 144,376 complaints various individuals had filed by May 2019. This should be seen in relation to the fact that effective legal enforcement in the area of data protection is likely to be difficult, costly, and time consuming for all parties involved (e.g., because checking the legal compliance of organizational data processing activities may require physical visits to individual companies and their digital backends) (see, e.g., Urban et al., 2018). For this reason, underfunded enforcement agencies across the EU might be taken as a sign of widespread political unwillingness among member states to enforce existing regulations effectively across their respective economies.

With regard specifically to data transparency and its potential to cultivate individual maturity, it is thus not apparent that regulators are or have until now been overly concerned with ensuring the realization of transparency's potential in this regard. While noting (as I did earlier) how GDPR has already on several occasions been mobilized effectively to hold big tech firms accountable, the present situation thus also indicates an unmistakable ceremonial aspect of "data transparency" for both regulators and organizations. For regulators, the widespread—albeit often ceremonial—enactment of new forms of data transparency among organizations might serve to create the appearance that new rules are effectively communicated, adopted, and enforced widely among organizations, even if this is not always the case. The ceremonial aspect extends to organizations as well, among which enactments of new forms of data transparency (i.e., updated privacy policies, consent interfaces, etc.) are more than likely to serve primarily as ways for organizations to demonstrate legal compliance and limit corporate liability, rather than necessarily entailing substantial changes to existing data processing practices (see, e.g., Calo, 2012; Meyer & Rowan, 1977). The point here is that data transparency could have a number of alternate purposes and functions for both regulators and corporate actors *besides* potentially cultivating individual maturity in the context of private-sector digitalization. A cynic might even go so far as to argue that the widespread ceremonial enactment of "data transparency" might be exactly what is needed to buffer the existing regime of surveillance capitalism *against* actual change and thus to preserve a version of the digital economy that—despite the prevalence of formal privacy policies and consent mechanisms—does exactly *not* allow individuals and publics to understand, opt out from, and/or meaningfully challenge the existing system (see, e.g., Zuboff, 2019; see also Birchall, 2021). In such a view, the primary purpose of data transparency would be exactly to consolidate organized immaturity as a social tendency, rather than meaningfully counteracting it (see, e.g., Brunsson, 2003, on "organized hypocrisy"). As the Snowden revelations illustrated, governments around the world have much to gain from the kinds of generalized, continuous surveillance made possible by digital technologies (e.g., for purposes of counterterrorism, national security, and population control), creating incentives for government that obviously contradict ideals of strict legal enforcement. Considering the relatively weak enforcement of GDPR and the noteworthy tendency toward

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

enactments of GDPR-mandated data transparency that facilitate the production of ignorance, manipulation, and loss of control by individuals of their data (rather than the opposite), such views, albeit cynical, seem to retain theoretical relevance. From the perspective of individuals, the observation that people often appear to "trust in surveillance" and/or make continuous use of the same technologies and digital platforms they claim to mistrust (see Whelan, 2019) is equally striking and important if we want to understand emergent forms of digitally facilitated (self-inflicted) immaturity. Future research, thus, might look into whether and under what circumstances data transparency is indeed envisioned and constructed with the intended purpose of cultivating maturity and consider situations when the purpose or function of transparency changes (e.g., when data transparency becomes perceived as merely a formal compliance exercise by organizations or a nuisance by individuals). Arguably, research might also consider situations in which data transparency becomes directly hypocritical as a means for organizations to intentionally mislead their stakeholders, as well as instances where such "deception" occurs unintentionally.

There are, of course, other possible and more optimistic explanations for the current levels of organizational (non-)compliance after GDPR and the risks this poses to the potential of data transparency to foster maturity, for example, the fact that the interpretation, translation, and implementation of new rules and norms (legal or otherwise) by organizations into practice take time and are not realized instantaneously (see, e.g., Christensen, Morsing, & Thyssen, 2013). Thus widespread practices of relatively ceremonial transparency measures that might at first occur as hypocritical might in fact be an early indicator of what will eventually occur as a more substantial change in organizational practices following GDPR, a process of change through which the potential of data transparency to cultivate maturity might be gradually realized. For example, what starts as a merely ceremonial enactment of "transparency" may over time come to morally entrap organizations as their stakeholders develop new expectations of what constitutes appropriate behavior (Haack, Martignoni, & Schoeneborn, 2021; Haack, Schoeneborn, & Wickert, 2012). As noted, there certainly are indications of market-wide changes in the behavior of not only European organizations but also, for example, websites originating in the United States after GDPR's enactment. On top of this, we are now witnessing the emergence of various non- or extralegal (i.e., private or public/private) standardization initiatives across the digital economy that in various ways aim at "responsibilizing" organizational behavior through, for example, organizational certification and labeling schemes (e.g., D-Seal, 2022; International Organization for Standardization, 2019; Swiss Digital Initiative, 2020). Whether and to what extent such initiatives contribute to guaranteeing the legal rights of individuals and the cultivation of individual maturity under digitalization, however, remain to be seen. This, too, thus, provides a potential avenue for future research, which might look into the temporalities of organizational implementations of various norms (legal or otherwise) of responsible behavior in the context of digitalization and personal data processing. Such research might consider instances in which such norm implementation effectively ensures qualities of individual maturity (e.g., enables the enlightenment,

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

autonomy, and reflexive self-determination of data subjects), as well as situations in which the cultivation of maturity fails or is counteracted by various conflicting interests and pressures. Of course, understanding comprehensively the role of data transparency vis-à-vis organized maturity and immaturity, respectively, including the perspective of individual data subjects, will likely be key to understanding transparency's possible and variegated effects in this regard.

For this discussion, it will also be essential to specify how and why the argument for the importance of cultivating maturity in the context of data processing may not be equally important in all conceivable contexts where something like individual maturity and immaturity are at stake and yet remains important in this specific context. That is, in the general context of modernity, one tends to be surrounded by technological and institutional systems to such an extent that it becomes quite impossible for each individual to understand let alone control each of them. For example, I might know very little about how the electricity grid or my car actually works and yet rely heavily on such technologies in my daily life. It might be impossible for me to understand the details of a surgery I am having, yet I choose to have it and might be likely to benefit from it. Thus, in the general context of modernity, it might seem unreasonable to suggest that people should only use technologies or receive surgeries they can fully comprehend to avoid the risk of "immaturity" altogether.

So why consider organized immaturity a threat worth acting upon in the specific context of surveillance capitalism? As put by Scherer and Neesham (2020: 15) with reference to Zuboff (2015), a noteworthy difference between surveillance capitalism and most other domains of modernity appears to be that the former mobilizes data-driven technologies to "[influence] individual behavior in non-transparent ways, for purposes that serve the interests of actors who are not accountable and largely operate beyond democratic control systems and the rule of law." In other words, the technological infrastructures of surveillance capitalism involve a set of opaque interests, hidden agendas, and socially illegitimate practices that, for example, electricity grids, medical surgeries, and car manufacturing generally do not (with the exception, perhaps, of "smart" vehicles). The fact that transparency provisions of new privacy-friendly regulation in practice tend to be reduced to additional means of producing organized immaturity rather than fostering maturity could indeed be seen as yet another example of and testament to the illegitimate practices of surveillance capitalism and its tendency to operate beyond both the law and democratic values. Furthermore, the fact that the quality of organizational data transparency mechanisms is becoming so deeply contested by surveillance capitalism at this current point in time, I would argue, points exactly to the potential of such mechanisms to directly contradict the logic of unlimited data accumulation if reconceived as effective safeguards to individual autonomy in the digital age. Thus the quality of data transparency now constitutes an important site of both socioethical and political struggle.

At this point, I will assume a deliberately normative standpoint with a mind toward practitioners engaged in the formulation and implementation of data transparency (including regulators and organizations alike). What is desperately needed, I

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

argue, are renewed and more sophisticated ethical appreciations of data transparency's complex—and, as I have shown, potentially problematic—implications for organized (im)maturity. Whereas the common understanding of transparency tends to assume a simple and strictly positive relationship between organizational enactments of transparency, on one hand, and the cultivation of forms of both individual enlightenment and empowerment, on the other, this article has served to illustrate and theorize transparency's potentially two-faced character in this regard, whereby data transparency may—under particular conditions—itself merely contribute further to the production of organized immaturity, rather than counteracting it. This is important because it implies that organizational enactments of data transparency will not automatically resolve the issue of organized immaturity under digitalization, even if such a promise is common in the typical rhetoric of data transparency. Indeed, as I have argued, new forms of data transparency might even contribute to rather than resolve the problem. This will especially be the case if the quality of new data transparency measures is left unattended by regulators and becomes the subject merely of organizational discretion and quick fixes (see Christensen, Morsing, & Thyssen, 2017). In such cases, data transparency risks turning into an additional source of the problem of organized immaturity itself.

The practical purpose of this article, thus, will have been to theorize the potentially problematic aspects of data transparency vis-à-vis organized (im)maturity so that we may more readily recognize, keep in mind, and deal with these potential problems in practice. For *regulators*—and other actors engaged in formulating organizational data transparency norms—recognizing the potentially two-faced character of transparency might help bring about more nuanced and critical understandings of 1) what practices of data transparency can realistically accomplish with regard to the cultivation of maturity under digitalization, 2) what the limits and even potentially counterproductive effects of data transparency might be, and 3) how to meaningfully address such limits or unintended effects through regulatory amendments, strengthened and/or targeted enforcement mechanisms, and so on.[3] In the case of GDPR-mandated data transparency, I have already pointed out such potential limits and counterproductive effects and have suggested possible ways to deal with them. Recognizing the potential limits and counterproductive effects of data transparency might make *organizations* concerned with the capacity of their data transparency practices to foster and sustain individual maturity—for example, by allowing individuals to understand as well as freely opt in to or out from data processing—realize

[3] I have already noted the potential need to require organizations both to disclose and to allow for user control of data-sharing connections with specific third parties. An additional way regulators might approach the issue of transparency and data subject control differently—and perhaps more effectively—would be to regulate *browsers* rather than individual websites. In the existing data economy, browsers function as a kind of gatekeeper that may largely determine the kinds of data websites can possibly collect. Requiring browsers to include a privacy dashboard through which data subjects may define preferred privacy settings *before* visiting individual websites would create a one-stop shop for individuals with regard to data control. Regulators, in turn, would have to ensure legal compliance only among a few browser providers rather than among millions of websites. As Cofone (2017) noted, however, European regulators have seemed hesitant with regard to this approach because most widely used browsers originate in the United States.

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

that personal data are currently being collected and processed in potentially illegal and/or unethical ways (e.g., without explicit individual consent). This might, in turn, inspire new and more appropriate transparency measures to ensure the legality and social legitimacy of data processing. For example, integrating various "privacy-by-design" technologies and continuously ensuring their functionality may be a valuable option. Such solutions should live up to—and might even surpass—existing legal requirements in terms of 1) ensuring user-friendly information provision based on a limited and specific set of terms, 2) allowing for an equal choice between accepting and rejecting tracking, 3) effectively blocking and preventing tracking until users have given their explicit consent, and 4) allowing for user control of any potential third-party data sharing. Stakeholder involvement might also be a worthwhile practice for organizations to determine when individual users experience data transparency measures as both informative and allowing for meaningful and free choice.

Finally, one might argue that the need to develop more sophisticated ethical appreciations of what constitutes meaningful transparency practices ultimately may require some measure of democratic deliberation. Here data transparency itself seems unlikely to foster the kind of critical public awareness needed for such deliberation to be meaningful. For example, we must recognize that data transparency is unlikely to display its own limitations and counterproductive effects. Thus, to foster critical public awareness of the role and efficacy of data transparency as a safeguard for individual maturity under digitalization, we need additional research, but we also need critical media attention and the attention of nongovernmental organizations, think tanks, and other such institutions concerned with public enlightenment. Indeed, increased public awareness of the existing challenges of enforcing GDPR in a sufficient manner and guaranteeing the rights of individuals in data-saturated environments might in itself strengthen the incentives of both regulators and organizations to prioritize these matters in the future. As this article (as well as much of the existing research on organizational data practices after GDPR) has suggested, even if new regulation has led to certain changes in organizational behavior, the current state of the digital economy appears to be quite far from what GDPR intended, including the degree to which individuals are guaranteed freedom from private-sector data processing to which they have not given explicit and informed consent. Raising public awareness about this fact and creating spaces for deliberation about how to meaningfully bring legal codes like GDPR into the future might not only constitute an important ethical endeavor at this time but could in itself provide new avenues for cultivating digital maturity within increasingly "data-driven" societies.

CONCLUSION

It is often assumed that new forms of regulatory data transparency (such as mandated by GDPR) provide an effective countermechanism to the organization of immaturity under private-sector digitalization. Transparency is claimed to do so by reinstituting the possibility of individual maturity—that is, individual

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

enlightenment, autonomy, and self-determination—in this context. This article has served to illustrate and theorize not only how data transparency's potential in this regard may be restricted but that such transparency measures themselves risk contributing to the production of new forms of organized immaturity under digitalization. Data transparency measures do so by systemically producing new forms of ignorance (e.g., forcing data subjects to make decisions based on terms they cannot reasonably comprehend), manipulation (e.g., pushing and/or nudging data subjects toward particular decision outcomes), and individuals' loss of control of personal data (e.g., limiting the technical and/or legal efficiency of the data subjects' consent decisions). Identifying these potentially dark sides of data transparency has allowed me to propose a set of potential remedies. Specifically, I have argued that what must be guaranteed to qualify data transparency as a means of restoring the possibility of maturity in the context of private data processing are 1) the contextual legibility of terms and information relevant to individual consent decisions, 2) the equality of choice options constitutive of these decisions, and 3) the overall efficiency of the individual's decision-making (whether technical or legal). Furthermore, I have argued for a general need to develop more sophisticated ethical appreciations of data transparency's—potentially problematic—relationship to organized (im)maturity. Regulators and organizations in particular should learn to recognize the potential limits and counterproductive effects of data transparency to better guarantee the quality of these measures in the future. This will be absolutely necessary to strengthen data transparency's potential for reorganizing maturity in the context of private-sector digitalization. Finally, developing public awareness of the current challenges with enforcing GDPR in a sufficient manner—for example, through research or critical media attention—may be a way of forcing both regulators and organizations to prioritize and attend to the quality of data transparency in the future.

Acknowledgments

The author expresses his gratitude to guest editor Andreas Georg Scherer and the three anonymous reviewers for their constructive approach and insightful comments. The author also thanks Mikkel Flyverbom and Lars Thøger Christensen for invaluable support in developing the final version of this article.

REFERENCES

Access Now. 2020. *Two years under the EU GDPR: An implementation progress report.* https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf.

Acquisti, A., & Grossklags, J. 2005. Privacy and rationality in individual decision making. *Security Privacy IEEE*, 3(1): 26–33.

Albu, O. B. 2014. *Transparency in organizing: A performative approach*. Frederiksberg, Denmark: Copenhagen Business School Press.

Albu, O. B., & Flyverbom, M. 2019. Organizational transparency: Conceptualizations, conditions, and consequences. *Business and Society*, 58(2): 268–97.

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

Angulo, J., Fischer-Hübner, S., Wästlund, E., & Pulls, T., 2012. Towards usable privacy policy display and management. *Information Management and Computer* Security, 20(1): 4–17.

Article 29 Working Party Guideline. 2018. *Guidelines on transparency under regulation 2016/679.* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

Berger, P. L., & Luckmann, T. 1991. *The social construction of reality: A treatise in the sociology of knowledge*. London: Penguin Books.

Best, J. 2007. *The limits of transparency: Ambiguity and the history of international finance*. Ithaca, NY: Cornell University Press.

Birchall, C. 2021. *Radical secrecy: The ends of transparency in datafied America*. Minneapolis: University of Minnesota Press.

Brandeis, L., & Warren, S. 1890. The right to privacy. *Harvard Law Review*, 4(5): 193–220.

Brunsson, N. 2003. Organized hypocrisy. In B. Czarniawska & G. Sevón (Eds.), *The northern lights—organization theory in Scandinavia*: 201–22. Copenhagen: Copenhagen Business School Press.

Calo, R. 2012. Against notice skepticism in privacy (and elsewhere). *Notre Dame Law Review*, 87(3): 1027–72.

Christensen, L. T., & Cheney, G. 2015. Peering into transparency: Challenging ideals, proxies, and organizational practices. *Communication Theory*, 25(1): 70–90.

Christensen, L. T., & Cornelissen, J. P. 2015. Organizational transparency as myth and metaphor. *European Journal of Social Theory*, 18(2): 132–49.

Christensen, L. T., Morsing, M., & Thyssen, O. 2013. CSR as aspirational talk. *Organization*, 20(3): 372–93.

Christensen, L. T., Morsing, M., & Thyssen, O. 2017. License to critique: A communication perspective on sustainability standards. *Business Ethics Quarterly*, 27(2): 239–62.

Cofone, I. N. 2017. The way the cookie crumbles: Online tracking meets behavioural economics. *International Journal of Law and Information Technology*, 25(1): 38–62.

Court of Justice of the European Union. 2019. *Panet49 GmbH v Bundesverband der Verbraucherzentralen und Verbracherverbände—Verbraucherzentrale Bundesverband e. V.* ECLI:EU:C:2019:801 (Case No. C-673/17). https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:62017CC0673.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. 2019. We value your privacy … now take some cookies. *Informatik Spektrum*, 42(5): 345–46.

Deleuze, G., & Guattari, F. 2013. *A thousand plateaus: Capitalism and schizophrenia*. London: Bloomsbury Academic.

D-Seal. 2022. *Denmark's new labelling program for IT-security and responsible use of data.* https://d-seal.eu/.

Eisenberg, E. M. 2007. *Strategic ambiguities: Essays on communication, organization, and identity*. London: Sage.

Erkkilä, T. 2012. *Government transparency: Impacts and unintended consequences*. New York: Palgrave Macmillan.

European Commission. 2016. *General data protection regulation GDPR.* https://gdpr-info.eu/.

European Parliament. 2020. *The CJEU judgment in the Schrems II case.* https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

Fenster, M. 2006. The opacity of transparency. *Iowa Law Review*, 91: 885–949.

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press

Fenster, M. 2015. Transparency in search of a theory. *European Journal of Social Theory*, 18(2): 150–67.

Flyverbom, M. 2019. *The digital prism*. Cambridge: Cambridge University Press.

Foucault, M. 2007. *Security, territory, population*. New York: Palgrave Macmillan.

Fung, A. 2013. Infotopia: Unleashing the democratic power of transparency. *Politics and Society*, 41(2): 183–212.

Fung, A., Graham, M., & Weil, D. 2007. *Full disclosure: The perils and promise of transparency*. Cambridge: Cambridge University Press.

Garsten, C., & de Montoya, L. 2008. *Transparency in a new global order: Unveiling organizational visions*. Cheltenham, UK: Edward Elgar.

Goldsmith, J., & Wu, T. 2006. *Who controls the internet? Illusions of a borderless world*. New York: Oxford University Press.

Haack, P., Martignoni, D., & Schoeneborn, D. 2021. A bait-and-switch model of corporate social responsibility. *Academy of Management Review*, 43(3): 440–64.

Haack, P., Schoeneborn, D., & Wickert, C. 2012. Talking the talk, moral entrapment, creeping commitment? Exploring narrative dynamics in corporate responsibility standardization. *Organization Studies*, 33(5–6): 815–45.

Hansen, H. K., & Flyverbom, M. 2015. The politics of transparency and the calibration of knowledge in the digital age. *Organization*, 22(6): 872–89.

Heald, D. 2006. Transparency as an instrumental value. In C. Hood & D. Heald (Eds.), *Transparency: The key to better governance?*: 59–73. Oxford: Oxford University Press.

Heil, O., & Robertson, T. S. 1991. Toward a theory of competitive marketing signaling: A research agenda. *Strategic Management Journal*, 12(6): 403–18.

Heimstädt, M. 2017. Openwashing: A decoupling perspective on organizational transparency. *Technological Forecasting and Social Change*, 125: 77–86.

Hood, C., & Heald, D. (Eds.). 2006. *Transparency: A key to better governance?* Oxford: Oxford University Press.

International Organization for Standardization. 2019. *ISO/IEC 27701:2019*. https://www.iso.org/standard/71670.html.

Irish Council for Civil Liberties. 2021. *Europe's enforcement paralysis: ICCL's 2021 report on the enforcement capacity of data protection authorities*. https://www.iccl.ie/wp-content/uploads/2021/09/Europes-enforcement-paralysis-2021-ICCL-report-on-GDPR-enforcement.pdf.

Jensen, C., & Potts, C. 2004. Privacy policies as decision-making tools: An evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*: 471–78. New York: ACM.

Kant, I. 1784. Beantwortung der frage: Was ist aufklärung? *Berlinische Monatsschrift*, 12: 481–94.

Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. 2020. The privacy policy landscape after the GDPR. *Proceedings on Privacy Enhancing Technologies*, 2020(1): 47–64.

MacKenzie, D. 2006. *An engine not a camera: How financial models shape markets*. Cambridge, MA: MIT Press.

Mayer-Schönberger, V., & Cukier, K. 2013. *Big data: A revolution that will transform how we live, work, and think*. Boston: Houghton Mifflin Harcourt.

McDonald, A. M., & Cranor, L. F. 2008. The cost of reading privacy policies. *I/S: A Journal of Law and Policy*, 4(3): 543–68.

Meyer, J. W., & Rowan, B. 1977. Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, 83(2): 340–63.

Mohan, J., Wasserman, M., & Chidambaram, V. 2019. Analyzing GDPR compliance through the lens of privacy policy. In V. Gadepally, T. Mattson, M. Stonebraker, F. Wang, G. Luo, Y. Laing, & A. Dubovitskaya (Eds.), *Heterogeneous data management, polystores, and analytics for healthcare*: 82–95. New York: Springer.

Nissenbaum, H. 2011. A contextual approach to privacy online. *Daedalus*, 140(4): 32–48.

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. 2020. Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI conference on Human Factors in Computing Systems*: 1–13. New York: Association for Computing Machinery.

Obar, J. A., & Oeldorf-Hirsch, A. 2018. The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication, and Society*, 23(1): 128–47.

O'Neill, O. 2002. *Autonomy and trust in bioethics*. Cambridge: Cambridge University Press.

O'Neill, O. 2006. The limits of accountability. *Accounting, Organizations, and Society*, 34(8): 918–38.

Pasquale, F. 2015. *The black box society*. Cambridge, MA: Harvard University Press.

Rawlins, B. 2009. Give the emperor a mirror: Toward developing a stakeholder measurement of organizational transparency. *Journal of Public Relations Research*, 21(1): 71–99.

Richards, N. M., & King, J. H. 2013. Three paradoxes of big data. *Stanford Law Review Online*, 66(4): 41–46.

Ringel, L. 2019. Unpacking the transparency-secrecy nexus: Frontstage and backstage behaviour in a political party. *Organization Studies*, 40(5): 705–23.

Roberts, J. 2009. No one is perfect: The limits to transparency and the ethic for "intelligent" accountability. *Accounting, Organizations, and Society*, 34(8): 957–70.

Roberts, J. 2018. Managing only with transparency: The strategic functions of ignorance. *Critical Perspectives on Accounting*, 55(C): 53–60.

Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P. A., & Santos, I. 2019. Can I opt out yet? GDPR and the global illusion of cookie control. In *Proceedings of the 2019 ACM Asia conference on Computer and Communications Security*: 340–51. New York: ACM.

Schackenberg, A., & Tomlinson, E. 2016. Organizational transparency: A new perspective on managing trust in organization–stakeholder relationships. *Journal of Management*, 42(7): 1784–810.

Scherer, A. G., & Neesham, C. 2020. *New challenges to enlightenment: Why socio-technological conditions lead to organized immaturity and what to do about it*. Working paper, University of Zurich and Newcastle University.

Stohl, C., Stohl, M., & Leonardi, P. M. 2016. Managing opacity: Information visibility and the paradox of transparency in the digital age. *International Journal of Communication*, 10: 123–37.

Strathern, M. 2000. *Audit cultures: Anthropological studies in accountability, ethics, and the academy*. London: Routledge.

Swiss Digital Initiative. 2020. *Our work*. https://www.swiss-digital-initiative.org/our-work/.

Tesfay, W. B., Hofmann, P., Nakamura, T., Kiyomoto, S., & Serna, J. 2018. Privacyguide: Towards an implementation of the EU GDPR on internet privacy policy evaluation. In *Proceedings of the fourth ACM international workshop on Security and Privacy Analytics*: 15–21. New York: ACM.

Thedvall, R. 2008. Transparency at work: The production of indicators for EU employment policy. In C. Garsten & L. de Montoya (Eds.), *Transparency in a new global order*: 143–60. Cheltenham, UK: Edward Elgar.

Trittin-Ulbrich, H., Scherer, A. G., Munro, I., & Whelan, G. 2021. Exploring the dark and unexpected sides of digitalization: Toward a critical agenda. *Organization*, 28(1): 8–25.

Trzaskowski, J., & Sørensen, M. G. 2019. *GDPR compliance—understanding the General Data Protection Regulation*. Copenhagen: Ex Tuto.

Urban, T., Tatang, D., Degeling, M., Holz, T., & Pohlmann, N. 2018. *The unwanted sharing economy: An analysis of cookie syncing and user transparency under GDPR*. arxiv.org/abs/1811.08660.

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. 2019. (Un) informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 ACM SIGSAC conference on Computer and Communications Security*: 973–90. New York: ACM.

West, S. M. 2019. Data capitalism: Redefining the logics of surveillance and privacy. *Business and Society*, 58(1): 20–41.

Whelan, G. 2019. Trust in surveillance: A reply to Etzioni. *Journal of Business Ethics*, 156: 15–19.

Whelan, G. 2021. *Megacorporation: The infinite times of Alphabet*. Cambridge: Cambridge University Press.

Zuboff, S. 2015. Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1): 85–89.

Zuboff, S. 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London: Profile Books.

. . .

Frederik Schade (fsc.msc@cbs.dk) is a PhD Fellow at the Department of Management, Society, and Communication at Copenhagen Business School. His research interests include the emergence of "digital responsibility" as a governmental and organizational norm as well as broader questions related to the challenges of societal mass digitalization.

https://doi.org/10.1017/beq.2022.30 Published online by Cambridge University Press