Journal of Business Research 122 (2021) 875–888

Contents lists available at ScienceDirect

Journal of Business Research

journal homepage: www.elsevier.com/locate/jbusres

Corporate digital responsibility

Lara Lobschat[a,*,ɪ], Benjamin Mueller[b,c,ɪ], Felix Eggers[d,ɪ], Laura Brandimarte[e], Sarah Diefenbach[f], Mirja Kroschke[a,g], Jochen Wirtz[h]

[a] School of Business and Economics, University of Münster, Am Stadtgraben 13-15, 48143 Münster, Germany
[b] Faculty of Business and Economics (HEC), University of Lausanne, Internef 134, 1015 Lausanne, Switzerland
[c] Institute of Information Systems and Marketing, Karlsruhe Institute of Technology, Kaiserstrasse 89, 76133 Karlsruhe, Germany
[d] Faculty of Economics and Business, University of Groningen, Nettelbosje 2, 9747 AE Groningen, the Netherlands
[e] Eller College of Management, University of Arizona, 130 E Helen St, Tucson, AZ 85721, USA
[f] Faculty of Psychology and Educational Science, Ludwig-Maximilians-University (LMU) Munich, Leopoldstrasse 13, 80802 Munich, Germany
[g] Etribes Connect GmbH, Wendenstrasse 130, 20537 Hamburg, Germany
[h] NUS Business School, National University of Singapore, 15 Kent Ridge Drive, Singapore 119245, Singapore

ARTICLE INFO

Keywords:
Corporate digital responsibility (CDR)
Digital technologies
Data
Ethics
Privacy
Organizational culture

ABSTRACT

We propose that digital technologies and related data become increasingly prevalent and that, consequently, ethical concerns arise. Looking at four principal stakeholders, we propose corporate digital responsibility (CDR) as a novel concept. We define CDR as the set of shared values and norms guiding an organization's operations with respect to four main processes related to digital technology and data. These processes are the creation of technology and data capture, operation and decision making, inspection and impact assessment, and refinement of technology and data. We expand our discussion by highlighting how to managerially effectuate CDR compliant behavior based on an organizational culture perspective. Our conceptualization unlocks future research opportunities, especially regarding pertinent antecedents and consequences. Managerially, we shed first light on how an organization's shared values and norms regarding CDR can get translated into actionable guidelines for users. This provides grounds for future discussions related to CDR readiness, implementation, and success.

1. Introduction

For the last couple of decades, digital advances have enabled a wide variety of systems with vast capabilities. Specifically, the benefits of automation, data analytics, artificial intelligence (AI), and machine learning to society are increasingly evident in daily life (Brynjolfsson & McAfee, 2017), and applications range from fulfilling consumer requests, making lending decisions, providing health advice, taking on high-risk jobs, protecting endangered species, to transporting people and goods (Wirtz et al., 2018). Yet along with this unprecedented power comes ethical dilemmas, in both consumer and business contexts, such as those associated with smart devices that constantly record data, the actions of autonomous vehicles in dangerous situations, and algorithms making recruitment decisions. Even if introduced with the best of intentions, malleable AI systems can be at risk of exploitation for unintended purposes (e.g., Nambisan, Lyytinen, Majchrzak, & Song, 2017; Richter & Riemer, 2013). It is the responsibility of system designers and the organizations that use these systems to recognize that their technologies may be used in ways other than they had anticipated with unwanted consequences for different stakeholders and society at large. However, existing research providing guidance for organizations in the face of ethical dilemmas related to the digital is scant.

In this sense, digital technologies that assist in human decision making or make decisions autonomously need to be subject to moral norms and ethical considerations similar to those that apply to humans. If we accept the premise that human behavior (individual and collective) should be governed by moral norms and ethical considerations, then any creation, operation, impact assessment, and refinement of

This paper is based on discussions at the Thought leadership Conference on Digital Business Models and Analytics at the University of Groningen in April 2018. We thank the organizers for their support.

* Corresponding author.
E-mail addresses: l.lobschat@uni-muenster.de (L. Lobschat), benjamin.mueller@unil.ch (B. Mueller), f.eggers@rug.nl (F. Eggers), lbrandimarte@email.arizona.edu (L. Brandimarte), sarah.diefenbach@psy.lmu.de (S. Diefenbach), m.kroschke@uni-muenster.de (M. Kroschke), bizwirtz@nus.edu.sg (J. Wirtz).

ɪ Lead authors. The other authors are listed in alphabetical order and contributed equally to the paper.

https://doi.org/10.1016/j.jbusres.2019.10.006
Received 15 July 2018; Received in revised form 3 October 2019; Accepted 3 October 2019
Available online 28 November 2019

digital technology and data should be assessed according to such rules. This argument presupposes that ensuring the ethical design and uses of digital technologies and related data is not solely a technological challenge (e.g., developing algorithms for ethical reasoning). Rather, it requires organizations to develop a comprehensive, coherent set of norms, embedded in their organizational culture, to govern the development and deployment of digital technology and data. We refer to this idea as corporate digital responsibility (CDR), defined as the set of shared values and norms guiding an organization's operations with respect to the creation and operation of digital technology and data. It requires tech companies, individual developers and designers, and any corporate actor employing digital technologies or data processing to be aware that the code they produce or deploy, as well as data they collect and process, inherently create an ethical responsibility for them. Consequently, organizations must determine how to operate responsibly in the digital age, while also complying with legal requirements and considering economic impacts on the organization (Schwartz & Carroll, 2003).

Our work in this article is pursuant of two complementary research objectives. First, we introduce the new concept of CDR, ask what the specific nature of CDR is, and how to conceptualize it. In our conceptualization and definition of CDR, we focus on the ethical issues that are unique to the digital context. Furthermore, we differentiate corporate *digital* responsibility (CDR) from corporate *social* responsibility (CSR) to highlight its distinctiveness while also drawing important links between the two. We identify key related stakeholders and key stages that CDR must address, namely, the creation, operation, impact assessment, and refinement of technology and data.

Next, second, we raise the question of how CDR can manifest in specific norms that effectuate CDR compliant behavior across levels. We approach this objective by employing an organizational culture perspective. This allows us to discuss the role of specific CDR norms in relation to artifact and behaviors. In the same vein, we sensitize decision makers to influences on and outcomes of CDR.

At the end, we synthesize our discussions by introducing a comprehensive framework that helps academics and managers build a CDR culture. Combined, our contributions support organizations in translating their mission and values regarding digital responsibility into actionable guidelines for users (i.e., managers, technology designers, and other employees).

2. Making a case for CDR

In the face of ethical challenges arising from the development and deployment of technology and data, organizations need to develop a better understanding of how to manage ethical dilemas and overall act digitally responsible. For this purpose, we turn to the concept of business ethics, broadly defined as the norms and standards that govern judgment and choices in business-related matters (Moriarty, 2016; Treviño, Weaver, & Reynolds, 2006). Based on the broad idea of business ethics, we define CDR as the set of values and specific norms that govern an organization's judgments and choices in matters that relate specifically to digital issues. Such CDR-related values and norms share some principles and goals with CSR, or an organization's commitment (and accountability) toward social and ecological causes in general. Accordingly, CSR encompasses the economic, legal, and ethical expectations that society has of organizations at a given point in time (Schwartz & Carroll, 2003), and we propose that a similar perspective is inherent to any considerations of CDR as well. Notwithstanding this similarity, we argue that CDR should be considered explicitly and separately from CSR, because of the particularities of digital technologies. To account explicitly for this difference, we highlight three characteristics that justify the explicit consideration of the digital, beyond an organization's wider social responsibility.

First, technological developments exhibit exponential growth (Moore, 1965). Building on the accelerated technological progress to date, the coming decades appear likely to produce even more disruptive innovations. According to Brynjolfsson and McAfee (2014), it is particularly recombinant growth among such innovations that requires corporations to face what the digital means. For example, big data and analytics are being combined with advances in machine learning and AI, allowing for the vast amounts of data already being collected to be put to even more efficient use.

Second, ethical and social concerns need to reflect the malleability of digital technologies (Richter & Riemer, 2013; Soltani, 2019). Social media were not created intentionally to spread fake news, but their algorithms, designed to maximize engagement, have contributed to this growing trend (Vosoughi, Roy, & Aral, 2018). From a corporate perspective (spanning from corporations that initially design and develop new digital systems to those that deploy them), digital responsibility thus entails a wide, complex, and highly dynamic set of moral challenges that cannot be exhaustively foreseen when a technology is designed or data initially captured, but that will only unfold in use over time.

Third, arguments that specific corporate norms are to deal with digital responsibility also derive from the pervasiveness of digital technologies. It has become nearly impossible to perform daily activities without the use of digital technologies, whether directly (using an app) or indirectly (an offline request gets processed by a digital technology in the background). Both corporations and consumers increasingly lack realistic options to lead their daily lives without digital technologies or avoid the potential effects of interrelated devices that track their behaviors.

Combined, these three aspects—exponential growth in technological development, malleability of technologies and data in use, and pervasiveness of technology and data—suggest that the *digital* is not just a linear development of previous technological advances but instead represents a quantum leap in digital technology that involves novel and specific challenges to corporations' ethical behavior that go beyond CSR. Nevertheless, CDR and CSR will likely prove complementary and overlapping (e.g., environmental impacts of digital technologies). This interplay is an important avenue for research; in this initial study, we focus on introducing and conceptualizing CDR as a foundation.

3. Basic framework of CDR, stakeholders, and stages

An ad hoc literature review reveals that in information systems research, eight leading journals have published only about 50 articles that broadly deal with ethical issues, following the first influential contribution in this vein in 1986 by Mason.[1] These articles cover heterogeneous topics, though without offering any concrete advice for specific CDR norms. Other academic disciplines touch on elements that are relevant to CDR (e.g., consumer privacy concerns, effects of human–computer interactions), and inside and outside business research domains (see Table 1).

While a full analysis and integration of these perspectives is beyond the scope of our efforts here, Table 1 illustrates that these isolated discussions have not produced a specific conceptualization of CDR in a business context yet. To address this conceptual gap, our engagement with these various domains and their relations to our own backgrounds and experiences leads us to propose a foundational framework of what CDR is and its role in organizations (Fig. 1). This framework includes four stakeholders that corporations must account for in their CDR efforts (Section 3.1), as well as four key stages linked to digital technologies and data, which mirror their lifecycles (Section 3.2).

[1] For our analysis, we used the *Senior Scholars' Basket of Journals* recommended by the Association for Information Systems. Details can be found at: https://aisnet.org/page/SeniorScholarBasket

Table 1
Role and Relevance of CDR in Key Disciplines.

Discipline	Role and Relevance of CDR
Marketing management	• Marketing scholars focus on balancing organizational data needs and customer responses (Lwin et al., 2007) and on organizational privacy failures, such as reputation risks related to hacking, data leaks, surveillance, profiling, and micro-targeting (e.g., Martin et al., 2017). • Service literature addresses the effects of service robots and privacy issues related to facial recognition, constant monitoring of consumers, decision making by AI (Van Doorn et al., 2017; Wirtz et al., 2018), and the vast amount of personal and transaction data captured by platform businesses such as Airbnb and Uber (Wirtz et al., 2019). • The Marketing Science Institute has made consumer privacy and the ethical discussions surrounding it a key research priority for 2018–2020.
Consumer behavior, consumer psychology, behavioral economics	• A focus on psychological privacy includes consumer privacy concerns and their antecedents, such as personality traits, knowledge, and experience (Malhotra et al., 2004). • Consumer privacy concerns evoke responses (e.g., Inman & Nikolova, 2017; Martin & Murphy, 2017; Wirtz & Lwin, 2009); studies also consider the relationship between privacy attitudes and privacy-related behaviors such as the privacy paradox and its mechanisms (e.g., cognitive biases; John et al., 2010; Kehr et al., 2015). • Privacy-related consequences include information disclosure and privacy protection behaviors (Son & Kim, 2008) • Key influencing contextual factors are the social context, control, and firm reputation (Steenkamp & Geyskens, 2006; Xie et al., 2006). • There is a trade-off of data provision and privacy risk with convenience, speed, personalization, and customization (Culnan & Bies, 2003; Smith et al., 2011; Wirtz & Lwin, 2009). Potential strategies to overcome consumers' privacy concerns include reducing privacy risk perceptions and increasing trust in the privacy policies and practices of an organization (Holtrop et al., 2017; Lwin et al., 2016; Schumann et al., 2014).
Human–computer interaction	• Investigations of the perceived role, influence, and responsibility attributions in human–computer interaction reveal the circumstances in which users blame computers for failed outcomes and unwanted effects (Hinds et al., 2004; Moon & Nass 1998) • Whereas the computer-as-tool paradigm sees technology as a tool extending human capabilities, the computer-as-partner paradigm sees technology as taking tasks delegated by the user through anthropomorphic means of communication (Beaudouin-Lafon, 2004), and the computers-as-social-actors paradigm indicates that people's responses to computers are fundamentally "social," such that they apply social rules, norms, and expectations that mimic those in interpersonal relationships (Lee & Nass, 2010) • Social robots, perceived character, and capability attributions lead to trust, over-trust, and under-trust (Ullrich & Diefenbach, 2017; Wirtz et al., 2018), such that people follow a robot's instructions in emergencies, though it actually performs poorly in navigation guidance (Robinette et al., 2016). In specific settings, people more readily follow a social robot's judgment than that of other humans (Ullrich et al., 2018).
Ethics, computer ethics	• Discussion of governmental privacy regulation and consumer data protection laws (Lwin et al., 2007; Sarathy & Robertson, 2003). • Analysis of privacy policies, transparency and fair data practices (Milne & Culnan, 2004) as well as cultural values and norms (Milberg et al., 2000). • Approaches to formalize ethical reasoning to enable computer-supported ethical decision making (Van den Hoven & Lokhorst, 2002). • Proposing models and approaches to moral or responsible design of digital innovation (Van den Hoven et al., 2014). • Development of alternative moral regimes for the information society (Floridi, 2010). • Discussion of specific ethical norms for autonomous systems (e.g., robots; Moor, 2006).
MIS, systems science, system design	• The focus of this literature is on ethical aspects of technology development and organizations' use of technology. • The impact of computer ethics of business-related IS research (Stahl et al., 2014) specifies impacts of technology on: o Organizational ethical behavior (Chatterjee et al., 2015). o Society at large (Avgerou & Madon, 2005; Lameijer et al., 2017). • Studies of the role of ethics in systems development and design cite: o Specific norms to guide system design (Chatterjee et al., 2009). o Abstract procedural guidance for developing and updating relevant ethical norms (Mingers & Walsham, 2010). • Digital ethics guide and define anticipation of (non)acceptable effects for users (Brey, 2012; Wright, 2011). • Special emphasis centers on the role of IT professionals (Oz, 1992; Walsham 1996). • Approaches ensure user and other stakeholder contributions in technology design processes (Olerup, 1989)
Design research, sustainability research	• Highlighting technology's influence on users in design, such as a moral gamification design framework (Versteeg, 2013). • Sustainable interaction design implies that design is "an act of choosing among or informing choices of future ways of being" (Blevis, 2007, p. 503), which relies on interactive technologies to promote more sustainable behaviors. • Recognition and discussion of unintended side effects of the digital transition – as well as rebound effects related to big data, AI, conversational software, digital biotechnology, and other technological advancements – as prerequisites for sustainable digital societies and environments (Montag & Diefenbach, 2018; Scholz et al., 2018).

3.1. Stakeholders

3.1.1. Organizations

Because organizations are the principal bearers of CDR, we expect specific CDR norms to develop at this level. Similar to other corporate-level frameworks (e.g., CSR), CDR provides organizations with a set of shared values and norms to guide their operations with respect to the creation and use of technology and data. In turn, other corporate actors, such as suppliers and partners and their digital technologies and data, must be considered. Various companies along the value chain develop or deploy digital technologies, and we explicitly note the importance of actors involved in software development or electrical engineering (e.g., semiconductors, communication networks, consumer devices, and apps), as well as settings that feature digital technology embedded into more traditional products or services (e.g., onboard computers in cars). The proposed conceptualization of CDR suggests a focus on a focal corporation, but we acknowledge the complex network of interdependent actors, beyond corporate boundaries, that are relevant ethical agents and critical stakeholders for digital technologies and data.

3.1.2. Individual actors

Even if organizations are the most direct addressees and bearers of CDR, the moral guidance offered by specific CDR norms also must effectuate CDR-compliant behavior across levels. To do so, the organization's mission and values must be translated into actionable guidelines for users (managers, technology designers, other employees), and

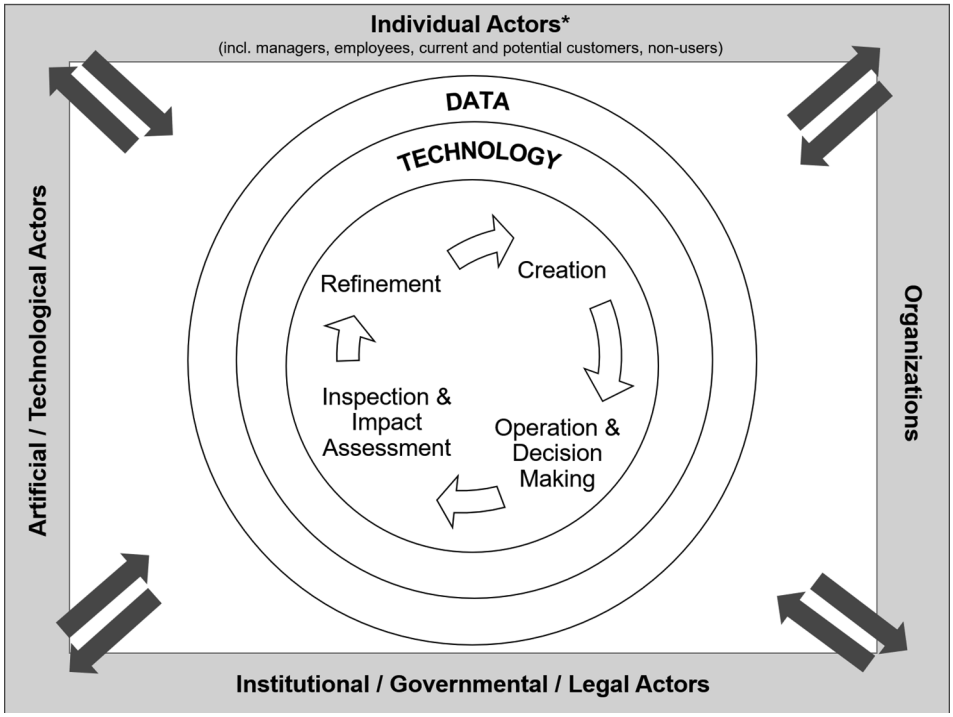

Fig. 1. Basic Conceptual Constituents of CDR. * The outer layer of the graph (in grey) contains CDR-relevant stakeholders.

those guidelines should be manifest in technological artifacts and behaviors. In this sense, institutions alone may be too abstract and collective to be effective, reliable bearers of ethical responsibility. We thus account for individual actors.

In a corporate context, managers are the principals that steer and account for their organizations, so they likely represent primary subjects of CDR on an individual level, followed by other employees. Thus, CDR also pertains to individual users (i.e., as agents of the corporation). Consequently, and beyond the immediate setting of a user employing a digital technology to do a task (which could be seen to rather suggest a concept like *personal digital responsibility*), we incorporate an interpersonal perspective into CDR. For instance, a user might interact with other members of the organization or beyond in technologically mediated ways (e.g., interactions through social media or input–output relations as in enterprise resource planning systems). Importantly, and though it may seem counterintuitive, we suggest that CDR also needs to take (potential) non-users of the technology into account to avoid lockout effects. For example, the creation and operation of digital technology and data can create a significant risk of exclusion (cf. discussions of the *digital divide*). In such settings, we see CDR as a principal vehicle to mitigate emergent "new forms of discrimination between those who can be denizens of [digital society] and those who cannot" (Floridi, 2010, p. 9).

3.1.3. Artificial and technological actors

We propose that CDR must acknowledge the existence of artificial actors. Despite their increasing relevance, such actors have not received much attention yet. The field of research into machine or robot ethics is relatively nascent (Crawford & Calo, 2016; Moor, 2006; cf. Van Wynsberghe & Robbins, 2018), referring mainly to actors' autonomous ethical reasoning. We suggest that CDR goes beyond that point, to include guidelines for the development and deployment of artificial and technological actors in an organization. Algorithmic decision-making, machine learning, and AI involve non-human and non-social entities, so a key question is whether and how we can delegate digital responsibility to artificial actors and take responsibility for their actions. Recent developments such as the recognition of socially biased algorithms (e.g., Wolfangel, 2017) and AI that can learn to write software code itself (Murali, Chaudhuri, & Jermaine 2018) highlight the need for ethical norms applied to artificial actors, such that CDR should be reflected in code and provide decision-making guidance to developers and algorithms.

3.1.4. Institutional, governmental, and legal actors

This category includes governmental or judicial entities (e.g., regulators and law enforcement) to which corporations are accountable in their approach to CDR. For example, the European Union's General Data Protection Regulation (GDPR) is an important legal framework for designing corporation-specific norms for CDR. Non-governmental organizations such as consumer and trade associations also can affect CDR (e.g., professional associations like the Institute of Electrical and Electronic Engineers (IEEE) with its code of conduct for software engineers).

3.2. Key lifecycle stages of digital technologies and data

In Fig. 1, we introduce four generic stages of the lifecycle of digital technologies and data, each of which is affiliated with key sources of ethical responsibility. In the interest of generality, Fig. 1 does not reflect any company-specific operations or particular processes per se. Rather, building on research into organizational knowledge processes (Intezari, Taskin, & Pauleen, 2017), we identify the (1) *creation of technology and data capture*, (2) *operation and decision making*, (3) *inspection and impact assessment*, and (4) *refinement of technology and data* as key stages that provide a better understanding of critical CDR-related issues related to digital technology and data. These main stages build on each other in a circular relationship.

Creation of technology and data capture refers to the initial stage in which new technologies are developed and data are collected. In the *operation and decision making* stage, the new technologies get applied and the data are put to work, such as to create customer profiles, to ultimately support decision making – whether by human or artificial actors, or a mixture thereof. The *inspection and impact assessment* stage features assessments of the resulting outcomes and captures how and to

what extent an organization relies on those outcomes in future instances of decision making. Finally, the *refinement of technology and data* stage relates to potential revisions of technologies and data, as well as the possibility of terminating an application or deleting data. In digital contexts though, a clear distinction of these main stages is difficult, because they tend to overlap (Nambisan et al., 2017). Nonetheless, we use these stages to analytically structure our discussion and identify potential ethical dilemmas and the related need for CDR when they appear most pertinent.

3.2.1. Creation of technologies and data capture

When creating any digital asset (development of technology, capturing data, training an AI), it is the responsibility of those designing and implementing the asset to ensure that this design and implementation embody ethical values. Consider software for example. Ethical norms need to inform its implementation, so the resultant systems behave in accordance with these norms subsequently. For instance, the design of a new machine learning algorithm must ensure the presence of transparency and accountability characteristics (which are particularly prominent in current debates). Similarly, designing data models for consumer data and models to analyze and predict should be guided by CDR norms, which then can help data scientists determine which data they can collect ethically and the conditions in which they can process that data.

This perspective on creation and capture does not apply solely to corporations that design and implement digital technologies and data models; it has powerful ethical implications for corporations that deploy and employ the digital assets, too. Organizations should include ethical considerations as criteria for their software selection and perform corresponding due diligence. Similarly, work with secondary data must consider the source of the data and the conditions in which it was generated (e.g., did users have a fair chance to offer informed consent for the collection and use of their data?). Legal frameworks provide important guidelines (e.g., GDPR), but a corporation needs specific engagement with CDR to develop a culture and norms that guide corporate behavior across levels. Thus, whether a corporation produces a digital asset or simply acquires one for deployment, this stage covers all corporate operations, from the initial ideation and design to the release of the digital asset for usage by others, internal (e.g., employees) or external (e.g., customers) to the corporation.

3.2.2. Operation and decision making

This stage covers all aspects related to the actual use of digital assets after their deployment. In this phase, digital technology and data are tightly intertwined in that the former is used to process the latter; while the latter shapes the processing of the former (e.g., machine-learning-based algorithms being trained on past data). Ultimately, we think of this stage as leveraging digital assets to inform or conduct decision making.

The stage of operation and decision making constitutes a multilevel phenomenon, spanning from corporate guidelines for how to use particular technologies and data to specific individual decisions related to their day-to-day use. An explicit emancipation of this stage is important from a CDR perspective because ethical responsibility cannot be assigned exclusively to those responsible for the creation of digital technologies and data.

This is particularly true because, as highlighted earlier, many digital technologies are not closed; they permit more than one form of usage, so corporations must recognize that technologies are malleable in use (Richter & Riemer, 2013). In particular, IT-based solutions are akin to universally reprogrammable machines (Moor, 1985), in constant states of flux, even after their release (Nambisan et al., 2017). Corporations thus cannot leave ethical responsibility only to those actors that create the digital assets, particularly when technology and data interplay tightly. Again, machine learning algorithms provide an example: results produced by the algorithm and decisions based on these results depend on the algorithm but also on the data used initially to train that algorithm. For instance, recent evidence indicates that using machine learning algorithms to support judicial processes or hiring practices can lead to the unintended projection of past race or gender biases onto future decisions if the algorithms are trained on historical data alone. Current data fed into such a system similarly would shape the future behavior of the system. Accordingly, CDR must sensitize corporations to the potential impacts and longer-term mutability of their digital assets in the operations and decision making stage.

3.2.3. Inspection and impact assessment

Organizations should critically assess the results operating digital assets and the decision making that occurs on that bases. This must include a broad perspective on the effects on all stakeholders, which involves both intended and unintended consequences of the decision taken. Generally, we assert that CDR norms must account for three perspectives. First, an assessment perspective should consider the beneficence of employing a corporation's digital assets. When generating and collecting user data, for example, an assessment of beneficence would require the corporation to determine whether the costs and benefits for users are balanced (Lwin et al., 2007). In turn, this requires that users learn about how the corporation is working with their data and are adequately compensated for allowing the corporation to do so (monetary or otherwise, such as enhanced convenience and customization). The multisided natures of many markets for digital products and services makes the assessment of beneficence for all involved stakeholders complex (Lwin et al., 2016), but specific engagement with CDR offers organizations an opportunity to adopt a clear approach to this challenge and involve relevant parties along their value chain.

Second, digital assets can have impacts beyond the stakeholders immediately concerned with their development and usage, especially platform and infrastructural technologies. For example, the emergence of wearable technologies and health apps likely will have implications for how health insurers calculate premiums, such that non-users might have to pay higher premiums (or be refused coverage) simply as a result of their unwillingness to share intimate health data, rather than any specific evidence that they live healthy or unhealthy lives. Specific norms for CDR thus need to account for such impacts which might extend beyond those in immediate contact with a corporation's digital assets.

Third, an impact perspective needs to account for the indirect and unintended effects of the creation and use of digital technologies and data. Many corporations are exploring whether blockchain technology offers opportunities for business model innovations, but few discussions reflect on the environmental impact of this new technology. Bitcoin alone, just one current blockchain application, requires electricity equivalent to that of 4.3 million average U.S. households annually to support its mining and trading systems, with corresponding environmental impacts. Such externalities call for a sense of ethical responsibility, which CDR's impact perspective must address.

Taken together, these perspective must inform a careful inspection of digial assets in terms of a critical review of their performance and impact. While this stage can also involve utilitarian goals (e.g., profitability, market share, etc.), we urge corporations that a true CDR perspective will require a careful and critical assessment of wider impacts as well.

3.2.4. Refinement of technology and data

Based on the insights that result from the inspection and impact assessment stage, and returning to the mutability of digital technologies and data, CDR norms should provide guidance for dealing with the inevitable changes to digital assets that are open and malleable in use. Continued engagement with digital technologies and data appears critical in this sense. For example, designers of machine learning algorithms should realize that the ethical responsibility for their creation

does not cease when the implementation stage is complete, and the algorithm has been shipped. Instead, CDR must involve ongoing engagement and monitoring; the corresponding norms might recommend transparency and accountability in all algorithms, to enable people who rely on them to understand how and why certain results arose. An ability to intercede into the decision-making process and correct unwanted outcomes should also be specified in CDR norms for review cycles and procedures or that define clear ownership and governance rules. Pragmatically, continued engagement also compels corporations to make sure digital technologies are patched and kept up to date, which can help mitigate the impact of emerging security threats.

As a special form of refinement, CDR norms must also cover the retirement of digital assets. Notably, CDR norms should specify how long collected customer data are kept on file, as highlighted in current discussions about the "right to be forgotten" on the Internet. Retirement considerations also apply to digital technologies per se, especially when these have become systemic or infrastructural, in that they set out ways to avoid being locked into a system as well as fail-safe conditions and procedures.

Table 2 provides an example that illustrate the four stages and discusses the potentially relevant ethical considerations that emerge in the respective context. In turn, these considerations need to be reflected in specific CDR norms that seek to guide and inform behaviors across levels

Synthesizing these discussions, Fig. 1 presents basic conceptual elements of a corporation's digital responsibility. The stages also constitute sources of digital responsibility relative to the digital technologies and data that a corporation's specific CDR norms should address. The answers need to reflect the context, expectations, and specific requirements that the four main stakeholders impose on a corporation's CDR norms. Only then can a set of specific norms guide the corporation's operations with respect to digital technology and data across all of the four stages we identify.

4. Toward a conceptual framework of CDR

With these four general stages of the lifecycle of digital technologies and data as conceptual building blocks of CDR, we seek to embed the concept in a corporate context to help decision makers better understand how CDR emerges and appreciate its potential effects. Beyond making the concept more accessible and concrete, this contextualization also should facilitate further research. Accordingly, we borrow from similar approaches (e.g., Homburg & Pflesser, 2000) to contextualize the influences on and effects of CDR according to organizational culture concepts. Specifically, we argue that culture provides a conceptual rationale for how CDR is shaped by and is able to shape corporate behavior. In line with Deshpandé and Webster (1989), we define organizational culture as "the pattern of shared values and beliefs that help individuals understand organizational functioning and thus provide them norms for behavior in the organization" (p. 4). In our research context, a CDR-related organizational culture, or *CDR culture*, describes the ways CDR is executed by an organization, which helps organizations become more knowledgeable about what CDR entails.[2]

4.1. Three layers of a CDR culture

Following Schein (2004), we posit that CDR culture exists at three fundamental layers (Fig. 2) that differ in their degree of accessibility and visibility to the observer but that also are strongly interrelated. These layers are *shared values, specific norms*, and *artifacts and behaviors*. The specific form of CDR culture relates to digital responsibility aspects of an organization and embodies assumptions and shared values (layer 1) from which specific CDR norms are derived (layer 2), which then result in specific artifacts and behaviors related to CDR (layer 3). Accordingly, we regard CDR norms as a form of applied ethics that influence employees' ethical behavior through formal and informal structures (Moriarty, 2016). The corporation's CDR culture must enable evaluations of alternative behavioral options and choices of the "right" way forward, on both individual and organizational levels.

4.1.1. Shared values supporting CDR within an organization

At the highest level of abstraction (layer 1 in Fig. 2), values represent what is considered desirable in an organization, manifested in its philosophies, strategies, and goals, which in turn are shared by all of its members (Schein, 2004). Unlike specific norms, shared values are not designed to guide behaviors in a specific CDR context; instead, they provide general guidelines for the development of specific CDR-related norms. For example, many organizations proclaim "respect for others" as a core value, which forms a basis for specific norms and informs context-specific behaviors.

To find general guidance regarding how to behave digitally responsibly, a long-standing discussion in computer ethics highlights the difficulties (Bynum, 2001), exacerbated because the fundamental shifts associated with the digital mean that "either no [moral or ethical] policies for conduct in these situations exist or existing policies seem inadequate" (Moor, 1985, p. 266). Rather than updating existing norms, CDR appears to need an entirely new underpinning. The uncertainty about which ethical norms apply (Rainie & Zickuhr, 2015) and the parallel existence of different views on adequate behavior, or norm fragmentation, likely induces conflict (Diefenbach & Ullrich, 2018). Corporations, therefore, are confronted with questions of whether established moral norms apply to their digital activities or if they need new norms, and if so, from whom, where, and how. In any case, their specific CDR norms differ with the moral grounds that provide their basis (e.g., deontological moral reasoning likely yields different CDR norms than utilitarian reasoning).

We do not seek to promote any specific set of values, but a few sources of inspiration might be helpful. On a general level, moral standards and responsibilities that might provide a foundation for a corporation's specific CDR norms could come from normative general human rights, as in the Declaration of Human Duties and Responsibilities (DHDR) or the Universal Declaration of Human Rights (UDHR)[3]. For example, Ashrafian (2015) proposes that if AI agents and robots receive human-based rights, they also must receive equivalent levels of duties and responsibilities. Beyond approaches based on normative general (human) rights, collections of specific ethical principles and values appear in studies of technological developments that identify key dimensions of moral guidelines. For example, Brey (2012) and Wright (2011) list some values that might guide a corporation's development of CDR norms.

4.1.2. Specific norms for CDR

With a higher degree of specificity than shared values, specific norms (layer 2 in Fig. 2) provide expression to an organization's shared values in a particular context (Feldman 1984). Using our previous example, the commonly shared value "respect for others" could translate into a specific norm such as "safeguard consumers' personal data" in a CDR context. Such specific CDR norms then should guide all activities by the organization in terms of what is right and wrong for the creation and use of digital technology and data (Maignan & Ferrell, 2004). For a business to be digitally responsible, its managers and employees must align their behaviors with specific norms established by the organization to achieve CDR. That is, specific norms make shared values explicit and tangible to effectuate CDR-compliant behavior across

[2] We thank the anonymous reviewer for this suggestion.

[3] Other ways to determine the moral conformity of ideals and actions exist, beyond such deontological approaches. However, for brevity, we limit ourselves to these illustrative examples.

Table 2
Activities and Potential Concerns in the Example of Wearable Personal Health Devices.

	Creation	Operation and Decision-making	Inspection and Impact Assessment	Refinement
Activities	Designing the wearable device (e.g., wristband) and deciding which sensors to use	Ongoing and continued collection of user data	Analyzing users' progress vis-à-vis their goals/ intentions	Refining analytics/algorithms (even re-training if need be)
	Building software and deciding which sensors of the host device (e.g., smartphone) to use	Analyzing user preferences and routines (e.g., exercise regime)	Assessing health advice	Refining decision rules; deciding when what recommendation is given to users
	Deciding which existing personal health data on the host device to use	Compiling data into comprehensive user profile	Analyzing customer complaints (e.g., on social media)	Implementing additional safety/security measures for users' data
	Building a data and prediction model for data analysis	Matching of user characteristics to other users based on selected variables	Inspecting algorithms and analytics to understand decision models	Deciding which new data need to be collected and which data need to be discontinued/deleted
	Capturing of data from the user	Probabilistically extrapolating unobservable data (e.g., future development of health) and future events (e.g., health incidents)	Benchmarking with technological progress and legisl/ation	Improving algorithms and predictive models
	Inferring health data from other sources (e.g., social media)	Making recommendations to the user on health-related issues	Assessing wider network of stakeholders (e.g., third-parties interested in data)	
	Deciding on storage location of data and data ownership		Analyzing of unintended effects (and ability to discover these)	
Potential Concerns	Users are not given fair chance at informed consent to collect data	Lack of transparency of data collection (e.g., which sensors) and analytics (e.g., why specific recommendations were made)	Lack of transparency in algorithms leaves systemic biases undetected	Right to "forget" not followed; data are kept without clear retirement dates
	Privacy concerns not considered	Lack of transparency and control to potential and current users about how data are used	Security concerns due to outdated technology or algorithms (e.g., data not stored securely)	Technology embodies sustained biases, discrimination, etc.
	Data accuracy not considered	Algorithmic decisions/recommendation lack validity (accurately reflecting underlying truth)	Lack of contingency governance (e.g., who owns data in case company is being bought)	Technology cannot be retired because data has become systemic (e.g., health devices required for insurance coverage)
	Over-collection of unrelated data (e.g., by using additional sensors in host device)	"Hidden agenda"/unrelated variables infused into analytics	Decisions/recommendations based on outdated medical advice	Data ownership changes without clear information to users (e.g., data acquisition)
	"Coerced" data provision by customer to gain customization, convenience, promotions		Unintended discrimination, biases (e.g., gender, ethnicity)	
	Safekeeping of data (data breach; hacking; identity theft)			

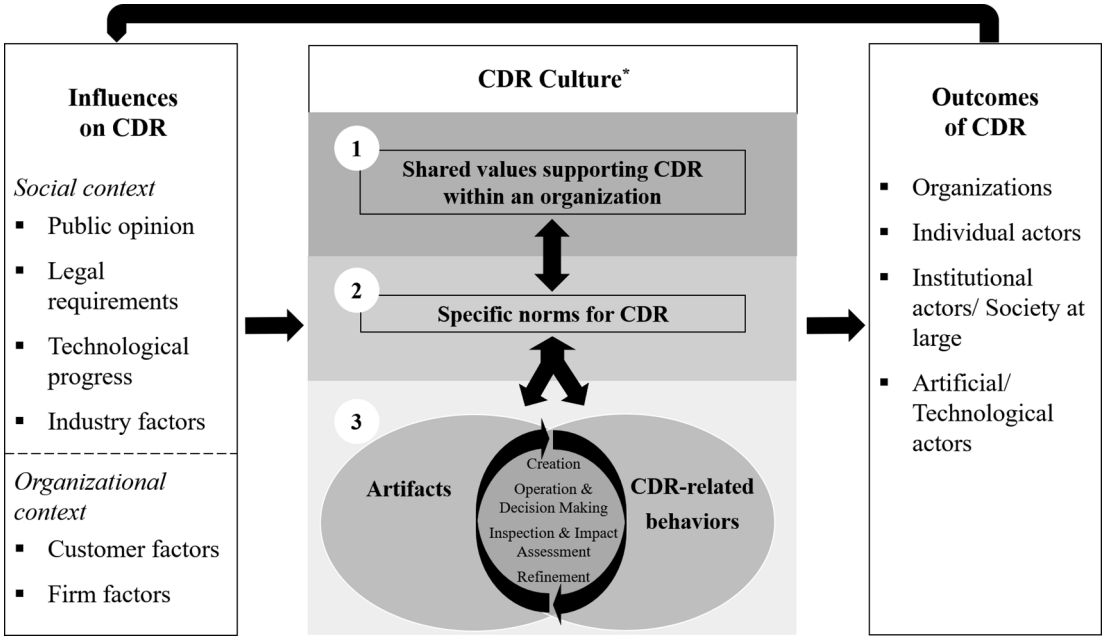

Fig. 2. Conceptual Framework of CDR. * Numbers 1–3 represent the layers of an organization's CDR culture, which differ in their specificity from a low degree of specificity (layer 1) to a high degree of specificity (layer 3).

organizational levels, so they help ensure the organization's mission and values get translated into actionable guidelines, which are especially important if conflicting interests and needs arise among different stakeholders (Maignan, Ferrell, & Ferrell, 2005). For example, customers might demand that their data are protected and stored in secure places without access to third parties, but the organization and its investors might prefer to share customer data with other firms to achieve strategic advantages or for profit reasons as exemplified by Facebook (Dance, LaForgia, & Confessore, 2018). Specific CDR norms, often manifest in a firm's mission or vision statement, can provide guidance for determining which stakeholder demands should take precedence (Maignan et al., 2005).

Clearly formulating and communicating specific CDR norms to all stakeholders of an organization (e.g., through official communication, websites, and annual reports) serves as a success factor for the implementation of CDR. As prior research shows, executives' activities and values exert strong influences on organizational consequences due to their high status in the organization (Finkelstein & Hambrick, 1990). It follows that top management commitment to CDR is important.

4.1.3. Artifacts of CDR

Values and norms are abstract structures; the elements of layer 3 in our framework are specific, concrete instances that embody commitment. The built technology itself is an artifact that must reflect and incorporate the corporation's CDR norms. Any digital artifact (e.g., technology, product, or service) becomes an instantiation of CDR. That is, acting with digital responsibility requires that the organization is not only aware of the various potential effects of the digital on consumers and society but also concerned for how its own actions may prompt such effects. Accordingly, CDR culture must establish that designers and creators of the technology bear responsibility for consequences that arise from its creation, operation, impact assessment, and refinement.

However, to transfer good intentions into action (i.e., ensure the corporation's CDR norms are manifest in the artifact), designers also have to consider the general claim of digital responsibility in their concrete design decisions and be equipped with strategies to do so. Returning to our example, the specific norm to "safeguard consumers' personal data" would require designers and programmers to implement encryption technology into products, even if it requires more computing power to deliver such products and services. Similarly, a prudent designer would instantiate this norm by designing models that only collect the amount of data necessary for the transaction in question. Beyond the creation step, corporations that adopt this norm would implement and enforce governance schemata that clearly define data ownership and responsibility, so the activity of safeguarding becomes more than a generic commitment.

In our framework, CDR artifacts have an important role and the power to shape existence and experiences (Ihde, 1990). Referring to technological artifacts, Verbeek and Kockelkoren (1998, p. 36) show that "technologies invite certain ways of dealing with them." Beyond the technological, artifacts such as corporate guidelines, documentation, process models, standard operating procedures, and handbooks provide instantiation to abstract values and norms (Pentland & Feldman, 2005). Defined process models prescribe a certain sequence of doing things that users draw on to plan their actions; software designs impose certain procedures and sequences to follow in order, to be able to transform inputs into desired outputs. Less manifest artifacts also can give substance to specific norms, such as stories, arrangements, rituals, and language (Homburg & Pflesser, 2000) or worldviews, goals, visions, expectations, plans, and myths (Astley, 1984). Overall, any such representation (D'Adderio, 2011) can help document, codify, and make explicit the corporation's CDR norms and the shared values on which they are based. Artifacts differ in their degree of prescriptive impact (e.g., corporate myths have less immediate impact on behaviors than a sequence of required data fields in a system interface), but they all shape (and are shaped by) individual CDR-related behaviors.

4.1.4. CDR-related behaviors

A corporation's specific CDR norms constitute applied ethics, in the sense that they inform action and support judgments and choices. Similar to artifacts, behaviors should instantiate a company's specific CDR norms and the shared values on which they are based. Layer 3 of the CDR culture framework thus comprises immediate, concrete outcomes in which CDR culture actually is manifested. For our exemplary "safeguarding consumers' personal data" norm, corporate and individual choices and judgments would need to reflect this norm. For example, the CDR norm would dictate that a client has the right to keep personal information private, and if the data is willingly shared, it

should be accurate and up to date. Business decisions would prioritize the primacy of this CDR norm over other motives (e.g., purely economic ones). Privacy is a critical trade-off that corporations face already, between benefiting from the increasing value of data and protecting individual privacy and data security (Tucker, 2012). Behaviors that pursue safeguarding consumer data would be reflected in corporate practices related to ownership and access to these data. This example also highlights the interplay of artifacts and behaviors: "Safeguarding consumers' personal data" requires a set of governance rules, roles, and responsibilities, which guide specific behaviors, which enact the embodied norms.

Therefore, CDR must determine which types of data should be captured or provided, under which conditions, how to collaborate with the data subject in updating or deleting them, and whether and how to share these data with third parties. In a data use context, CDR can define the purposes for which the data were originally collected and enforce policies to avoid unintended and unauthorized uses. Ensuring fair data uses and exchanges is a core challenge for the evaluation of the impacts of data creation and use policies. For example, when defining such policies, corporations might consider whether to use purchasing or behavioral data to target advertisements or price discriminate and whether to use photos posted on social networks to train facial recognition algorithms. Have any issues emerged, with customers or regulatory institutions? What costs did or will the corporation incur? Answering such questions can support policy refinement and creative approaches, such as considering the possibility of storing data in aggregate form only for a limited amount of time.

4.2. Influences on a CDR culture

To provide insights into the constituents that influence an organization's CDR-related decision making and CDR culture, we take a stakeholder approach (Yang & Rivers, 2009). Consistent with Yang and Rivers (2009), we differentiate stakeholders from social contexts, including public opinion, legal requirements, technological progress, and industry factors, and those from organizational contexts, such as customer and firm factors (which include employees).

4.2.1. Public opinion

Social pressure can vary in its time perspective (short- vs. long-term) and channels, such as social media or the international press (Hoppner & Vadakkepatt, 2019). Social media offer vast platforms for sharing ethical dilemmas pertaining to CDR-related practices with large audiences of consumers within seconds, which can exert immense pressure on organizations to accede to stakeholder demands. Furthermore, data privacy is a great risk in digitized settings (Solove, 2005); recent data breaches involving large corporations (e.g., Equifax, Target, the U.S. Office of Personnel Management) and exposures of controversial data-sharing practices (e.g., Facebook data acquired by Cambridge Analytica in breach of terms and contracts) have sensitized the public to the importance of proper data management and its consequences (CNN, 2013; Granville, 2018; Koerner, 2016; The Economist, 2017).

In this sense, companies should realize that their key long-term asset is not customers' data alone but in combination with customers' good will and social capital. If they wish to avoid boycotts like the #deleteFacebook debacles or costly litigation, they must consider the serious responsibilities associated with receiving people's personal data. Furthermore, if social networks provide platforms for users to share user-generated content, public debates (and media coverage) will focus on their responsibility to control and (if applicable) proactively filter inappropriate content, such as racist language or live broadcasts of violent crimes (Isaac & Mele, 2017). An ongoing debate also questions whether violent video games represent a potential catalyst of mass shootings, increasing the social pressure on software firms to account for such ethical considerations when designing video games (Salam & Stack, 2018). In an AI context, public discussions about racial discrimination prompt calls for "algorithmic accountability" in applications such as facial recognition, health care decision making, and identifying reoffenders in judicial systems (Lohr, 2018). Growing salience of ethical issues in society at large will increase the social pressure on organizations to engage in CDR.

4.2.2. Legal requirements

Of the many dimensions of CDR, data management actually features some well-defined guidelines, reflecting existing laws and regulations. However, because these regulations are country-specific, they pose challenges to multinational corporations. Even with universally accepted guidelines for data security (ISO/IEC, 2013), data privacy suffers from less standardized practices, largely because it is hard to define; what should be kept private varies across cultures, individuals, and times (Acquisti, Brandimarte, & Loewenstein, 2015; Moore, 1984). As a consequence, countries have enacted vastly different legal frameworks for data privacy. On one end of the spectrum, the European Union's centralized approach is characterized by strong regulations that treat any personally identifiable data as a valuable asset, under the control of the individual (Council of the European Union, 2016). The recently released GDPR aims to harmonize data privacy laws across Europe and reshape organizations' approach to data management, by prioritizing individual protections. At the other extreme, the decentralized, deregulated U.S. approach to privacy protection treats different data differently and mostly allows corporations to self-regulate. This latter approach reflects fair information practice principles and general guidelines (FTC 2012). Harmonizing the legal practices surrounding data creation, usage, assessment, and refinement thus is challenging, especially internationally, with notable implications for the development of an organizational CDR culture. For example, substantial legal distance between countries in which an international organization operates might force it to adopt local artifacts and CDR-related behaviors, while maintaining its overall shared values and CDR-specific norms.

4.2.3. Technological progress

Much of our earlier discussion on the characteristics of the 'digital' highlights that CDR culture is also influenced by technological progress. In particular, the three characteristics we discussed earlier – exponential growth, malleability in use, and pervasiveness – highlight why contemporary technologies and their progress constitutes a special influence on corporate efforts to ethically govern their engagement with digital technologies and data. It will be difficult to spell out any functional or even deterministic impacts of levels or kind of technological progress on CDR. However, technologies such as machine-learning algorithms with large amounts of digital data at their disposal that require little human supervision or intervention make ethical concerns more pressing and of a different nature than the use of more traditional corporate computing (e.g., ERP or CRM system).

4.2.4. Industry factors

The industry in which an organization operates and the products it markets influence the importance of CDR and the extent to which that organization responds to CDR expectations with relevant organizational practices (Hoppner & Vadakkeepatt, 2019). For example, if the organization's business model already depends on digital technology and data usage (e.g., AirBnB, Google; Wirtz et al., 2019), it will likely confront substantial CDR-related expectations immediately. This holds especially true for industries like the medical industry where very sensitive patient data is collected and processed via digital technology hence increasing the likelihood of ethical dilemmas. For these organizations, establishing a CDR culture is instrumental.

In contrast, other industries which still await larger impacts of digitalization, CDR may be less of a pressing issue (Wade 2017). For this latter group, coping with ethical issues and engaging in CDR practices may appear less urgent, even though prudent foresight would encourage such corporations to get ahead of the curve. Such CDR-related

expectations are fueled by public opinion, and competitive behavior, beyond cross-industry differences, might also play a crucial role. For example, if selected industry players engage in CDR (first-mover advantage), it might become a benchmark that forces others to live up to these "newly established" CDR industry standards.

4.2.5. Customer factors

In its data management, a digitally responsible corporation addresses customer concerns about security and privacy (Lwin et al., 2016). As we discuss subsequently in the legal requirement section, well-established standards exist for security policies. However, defining privacy policies is more challenging because of the inherent tension between profit maximization through data use and protecting customers' privacy.

Information systems research provides some guidelines by identifying factors that affect people's privacy concerns (Smith, Dinev, & Xu, 2011), including those that affect the rational evaluation of risks and benefits associated with sharing personal data (i.e., the privacy calculus; Klopfer & Rubenstein, 1977; Stone & Stone, 1990), emotions, and psychological and behavioral biases that go beyond an economically rational process of utility maximization (Dinev, McConnell, & Smith, 2015). In detail, such factors might reflect personal experiences of privacy incidents (e.g., identity theft, discrimination based on personal data), general awareness of privacy risks, personality/demographic differences, and trust in the corporation, as well as cognitive biases, heuristics, affect, and time constraints.

Each organization should consider which benefits (and risks) its customers perceive when they provide personal data to evaluate the significance of data privacy for them. For example, consumers who strongly value their personal privacy and perceive an organization's data collection or use as invasive might not agree and even could voice their concerns openly to other potential and existing customers. Consequently, customers' position in the power balance with the organization also should be taken into account (Greenaway, Chan, & Crossler, 2015). From a more positive perspective, organizations could construct a strong CDR culture by emphasizing its digitally responsible organizational behavior, as a source of competitive advantage (Porter & Kramer 2006). Using customer information to set up an appropriate CDR culture thus can create win–win situations for customers and the organization.

4.2.6. Firm factors

Corporations face an important trade-off when defining their CDR strategies: By engaging with customers to provide a product or a service, they gain access to valuable (more or less sensitive) data about customers' demographics, habits, interests, likes, financial and health situation, and so on. If shared with or sold to third parties, such a treasure trove of data could easily be turned into profit. Yet, a digitally responsible corporation would recognize its customers' privacy rights (consumer factors), which limit the uses of those data. Examples of this trade-off are relevant to targeted advertising (Tucker, 2012), product customization (Lee, Ahn, & Bang, 2011), and enhanced service convenience (Lwin et al., 2007).

In theory, targeting, customization, and enhanced convenience benefit the organization and its customers. For example, the corporation increases the chances that its promotion will prompt a purchase, because the advertised offer matches the needs of the customer better, and the customer receives information about an appealing product or service that is aligned with her or his interests. In practice though, organizations often fail to be transparent about how they use the data that customers share with them. Advanced data gathering and tracking technologies, and the lack of clear or well-enforced regulations (legal requirements) also allow data to be collected without customers' knowledge or explicit and informed consent. In other situations, they obtain consent simply by imposing practices to customers without making the option to refuse those practices clear. In such contexts, the organization's reputation and customer trust will strongly influence its CDR strategy.

In particular, organizations that suffer from a low level of trust and reputation are likely to experience more external pressure to establish a strong CDR culture than organizations with high levels of trust. The strong CDR culture then could issue a (positive) signal that the organization has taken responsibility for its technology and data-related actions, which may improve its trust and reputation. From a more strategic perspective, organizations with high reputation levels potentially might leverage opportunities to develop a CDR culture to provide (social) welfare and gain additional competitive advantages. Moreover, its competitive positioning will determine the extent to which ethical dilemmas related to technology and data will be salient and influence the firm's CDR-related decision making (Porter & Kramer, 2006).

In addition to contextual factors, leadership and staffing influence CDR-related decision making. Consistent with CSR research (Godos-Díez, Fernandez-Gago, & Martinez-Campillo, 2011), we predict a strong impact of the CEO's ethical engagement on the organization's CDR culture. An ethically involved CEO will sometimes sacrifice corporate profit considerations for CDR matters, which can foster the development of a strong CDR culture that comes to life across all departments of the organization. Then, the organization's employees determine the CDR culture in that the more involved they are, the more likely the organization will respond to internal pressures to address ethical dilemmas by establishing a CDR culture (Yang & Rivers, 2009). In terms of privacy, employees might sense the need to protect their own personal information and demand that the organization take action by establishing a CDR culture. Finally, employees' positive attitudes toward CDR should encourage a CDR culture that considers other stakeholders' positions.

4.3. Outcomes of a CDR culture

Corporate responsibility initiatives can be challenging to implement because they require the coordination of various stakeholders, entail high costs and complex implementation efforts across the corporation's various functions, require significant time to induce deep changes to corporate and individual behaviors, and produce difficult-to-calculate monetary returns. Similar, challenges apply to CDR initiatives such as organizational privacy programs (Culnan & Williams, 2009). The returns only arise in the long term, such that it may be impossible to justify CDR activities simply on the basis of their financial returns. Instead, it is necessary to examine CDR benefits and costs for various stakeholders, including individual actors (consumers), institutions, governments, the legal system, and artificial and technological entities. We tentatively review some of the outcomes of CDR relative to these stakeholders from our framework (Fig. 1).

4.3.1. Organizations

Implementing a CDR culture can be costly for organizations, especially in the short term, as is illustrated by privacy protection projects that demand security investments and reduce or at least limit financial gains from selling data. Just as consumers face trade-offs (costs and benefits) from their data disclosure, so do corporations (organizational privacy calculus; Greenaway et al., 2015). Applying a digitally responsible approach to technology development and deployment requires corporations to incorporate ethical questions into their investment decisions (Marshall, 1999), such as those pertaining to refinement and retirement. Yet such questions may be hypothetical in nature, so the organizational actors (e.g., corporation acquiring a new technology, technology companies providing it) need to document their predictions of future developments (e.g., complementary technologies, use-related mutability of technology). Monitoring whether these assumptions hold true and the potential implications of their violations represent ongoing activities with far-reaching consequences for how corporations use digital technology and data.

Corporations must determine their CDR-related obligations to their customers and choose a CDR strategy that suits their business model by balancing value creation and value appropriation. Moreover, they need to note the potential negative consequences of neglecting their digital responsibility relative to the investment costs they incur by establishing and nurturing a CDR culture[4]. Prior research shows that privacy breaches and security incidents result in significant losses in reputation and firm value (Acquisti, Friedman, & Telang, 2006; Martin, Borah, & Palmatier, 2017), as well as the risk of penalties enforced by governmental authorities like the U.S. Federal Trade Commission. Organizations would be well-advised to consider these potential (extra) costs when deciding if and to what extent they want to become digitally responsible. In parallel, they might strategize to use their implementation of CDR not solely as a loss prevention tool but as a competitive advantage to achieve stronger financial performance in the long term. Analytics advances provide some previously unavailable solutions, such as supporting the derivation of useful managerial implications, even without individual-level data (Holtrop, Wieringa, Gijsenberg, & Verhoef, 2017; Wieringa et al., 2019).

Beyond these (short-term) financial considerations, we expect organizations implementing a CDR culture to experience (long-term) positive financial impacts due to positive indirect performance effects that move through upstream performance outcomes (Saeidi, Sofian, Saeidi, Saeidi, & Saaeidi, 2015). Consistent with CSR research, we expect an organization's CDR culture to increase customer satisfaction and competitive advantages (Saeidi et al., 2015), customer trust and loyalty, and firm reputation (Stanaland, Lwin, & Murphy, 2011). Eventually, these effects should improve an organization's financial performance (Saeidi et al., 2015). In line with Chahal and Sharma (2006), we also anticipate that a CDR culture will enhance the organization's brand equity and competitive positioning in the market. As a type of corporate social performance, CDR should reduce the cost of capital, which can help justify CDR investments (Agarwal & Berens, 2009).

4.3.2. Individual actors

Not all consumers have the same privacy preferences. Some consumers do not value their privacy highly and are willing to exchange personal data for even small rewards (Athey, Catalini, & Tucker, 2017). Others care deeply about privacy but still share their personal data with companies because they value the services, enhanced convenience, and customization they receive in return (Beke, Eggers, & Verhoef, 2018; Ghose, 2017; Wirtz & Lwin, 2009). Perhaps the majority of users cannot determine if a transaction is worthwhile, whether because they are not aware of or do not understand the actual, practical costs and benefits associated with a data transaction. The difficulty of reading and understanding privacy policies (McDonald & Cranor, 2008) and the complexities of the data market—in which first, second, and third parties, advertising networks, and data brokers buy and sell personal data—suggest it may be impossible for individual laypeople to make informed decisions about their true willingness to share their personal data. Even if they devote greater effort to understand the costs and benefits involved, they face inescapable limitations, ingrained in human nature, such that behavioral and psychological biases make it impossible to achieve perfectly rational decisions when it comes to sharing personal data (Adjerid, Acquisti, Brandimarte, & Loewenstein, 2013; Brandimarte, Acquisti, & Loewenstein, 2013).

Transparent CDR guidelines might ease this decision-making process, as well as reduce reactance (White et al., 2008) and ultimately increase trust. For example, Aguirre et al. (2015) show that consumers are less likely to click on online ads if corporations engage in covert information collection and use that information for personalized targeting without informing customers about the collection. If the targeting reflects collected data that consumers were previously unaware of disclosing to the corporation, those consumers might feel unfairly treated and perceive a violation of normative standards of openness and permission (Ashworth & Free, 2006).

Similar to CSR findings, we expect that an organization's CDR culture will result in both functional and psychological benefits for customers, especially if the ethical issues being addressed are relevant to them (Bhattacharya, Korschun, & Sen, 2009). An organization's CDR culture can encourage customer–company identification (Homburg, Stierl, & Bornemann, 2013) and positively affect customer outcome measures such as satisfaction, trust, and loyalty toward the organization (Saeidi et al., 2015).

Beyond this customer perspective, CDR norms and culture constitute a form of applied ethics that guide individual behaviors within the corporation. Individual users may find it alien to think of their uses of digital technologies as having long-term impacts, even though each usage instance has notable consequences. Accordingly, considering CDR on the individual level may have strong implications for users' reflexivity about their uses, according to the relationship that exists between the user and the technologies s/he uses. Rather than simply applying a machine learning algorithm to speed up decisions, individual users might be required to think about whether their decision is in line with corporate goals and relevant ethical guidelines. Such CDR norms and culture then should have wide-ranging consequences for how people work with digital technologies and data, in a digitally responsible manner.

4.3.3. Institutional actors and society at large

Although abstract, this aspect likely accounts for the most wide-ranging outcomes of CDR. Societal discourse on CDR likely will prompt political actions to implement and frame high-level agreements about a digitally responsible future. Along with the EU's GDPR, such frameworks promise notable consequences. Efforts to tax corporations appropriately (whatever that means) when their business models rely on data offer another example. Proposals to tax robotic work that substitutes human labor, based not on the capital employed but rather on the work done, reveals a consequence of CDR that transcends the corporate level.

The way that organizations approach CDR also may have implications for society. We suspect that current hot-button issues (e.g., fake news, hate speech, and echo chambers) would be strongly influenced by CDR.

On a more general level, CDR can shape daily lives. Technological advances already influence how languages change, how we interact, and other social factors. Accordingly, CDR plays a key role in pursuing what we discussed earlier: future developments that are not only guided by the technologically feasible, but also by what is societally desirable and sustainable. This is also a good example for the feedback effect (see Fig. 2) we expect from CDR outcomes to influences on organizations' (future) CDR-related decision making.

4.3.4. Artificial and technological actors

Exciting organizational and technical consequences of CDR are likely to involve artificial actors and technology. If CDR is implemented by a corporation, can its spirit consistently govern the behavior of artificial actors? Organizationally, updated governance schemes and new roles will be required to ensure adherence to CDR norms. Ongoing engagement with any digital technology, once created, requires the instigation of corresponding roles, tasks, and processes, along with recognition and rewards for the respective behaviors and sanctions for negligence. Software development methodologies might need to be updated to reflect consistent guidance by the ethical principles spelled out in the corporation's CDR norms. Technologically, the current debate hints at increasing transparency and accountability in algorithmic decision making. We expect CDR to be highly consequential in this domain. Beyond policing their behaviors, AI agents may be used

[4] We thank the anonymous reviewer for this suggestion.

increasingly to ensure other individuals' behaviors remain in line with corporate policies, such as monitoring usage behaviors and preventing unintentional data leakages (Hadasch, Li, & Mueller, 2013). Such options can improve data protection and privacy, as well as enforce specific CDR norms more directly.

5. Implications for academia, management practice, and society

With this conceptual article, we aim to set a cornerstone and stimulate academic research about CDR as well as provide initial guidance to practitioners interested with CDR. As outlined, CDR is hard to define; our discussion does not claim to be comprehensive or definitive. Rather, we aim to provide a catalyst for an integrative, interdisciplinary research effort to develop useful insights pertaining to this multidimensional, dynamic concept. As we have suggested, multiple research avenues clearly arise, pertaining to understanding and analyzing the nature, drivers, and outcomes of CDR for business scholars.

Perhaps the most critical question though is the impact of CDR on the focal organization and its stakeholders. We anticipate a positive relation of CDR with an organization's competitiveness and financial performance, but conceptual and analytical models should assess this outcome explicitly. Such approaches would facilitate managerial decision making about CDR initiatives. Considering the different stages and stakeholders involved in CDR, its measurement will be challenging and likely require multidimensional scales, together with multiple monetary and non-monetary performance measures. A (non-exhaustive) list of research questions with the potential to extend thinking about opportunities and challenges related to CDR includes:

- Which theoretical approaches and models can help build a robust understanding of how individuals, organizations, and society behave digitally (ir)responsibly?
- How can organizations balance the trade-off of ethical norms and moral obligations with pressures to increase efficiency and profit by creating new systems and data?
- How should we capture and assess an organization's CDR readiness and degree of CDR implementation?
- How can organizations successfully communicate a CDR culture to its employees and incentivize them to also be committed towards the CDR culture?
- How does a CDR culture influence consumer reactions, including perceptions (e.g., benefits, concerns), feelings (e.g., trust, commitment), and behaviors (e.g., usage, loyalty, and engagement)?
- How can organizations differentiate themselves and create a competitive advantage by implementing a robust CDR culture?
- When do changes in the internal and external environment posit the need to update an organization's CDR culture?

We call on executives to establish strong corporate CDR cultures and develop corresponding norms and guidelines for their employees. Even in settings in which implementing specific CDR norms may appear ineffective, an increased emphasis on ethical reflection can influence future behaviors positively, both with regard to technology development and deployment, as well as data privacy. A similar logic applies to corporate and organizational contexts, as well as in the domains of public discourse and policy.

According to our conceptualization, corporations should not rely on legal and regulatory guidelines alone to address emerging digital challenges. Such guidelines typically cannot keep up with the speed of technological progress. Rather, corporations should embrace a comprehensive set of CDR-related principles and processes to address stakeholder demands and secure their support, which requires both strategic and operational decisions and processes. On a strategic level, organizations should develop and define their CDR-related mission and vision. At the operational level, they need appropriate tools, techniques, processes, and structures to implement their general strategic view. The multidimensional role and diversity in the nature of CDR likely requires changes through the entire organization, including organizational restructuring, training and development of employees, and implementation of new processes (e.g., data management, communication).

In summary, this article introduces the important concept of CDR, with the promise of opening a new research field. Contemporary CDR questions are widespread, spanning consumer, organizational, and societal aspects; continued work in this field is important and urgently needed.

References

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

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. ICIS 2006 Proceedings, 94.

Adjerid, I., Acquisti, A., Brandimarte, L., & Loewenstein, G. (2013). *Sleights of privacy: Framing, disclosures, and the limits of transparency. Proceedings of the Ninth Symposium on Usable Privacy and Security (Article No. 9)*. ACM.

Agarwal, M.K., & Berens, G. (2009). How corporate social performance influences financial performance: Cash flow and cost of capital. MSI Working Paper, 09-001, 3-26.

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing, 91*(1), 34–49.

Ashrafian, H. (2015). Intelligent robots must uphold human rights. Nature, Available at https://www.nature.com/news/intelligent-robots-must-uphold-human-rights-1.17167 (Accessed: March 18, 2019).

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics, 67*(2), 107–123.

Astley, W. G. (1984). Subjectivity, sophistry and symbolism in management science. *Journal of Management Studies, 21*(3), 259–272.

Athey, S., Catalini, C., & Tucker, C. (2017). The digital privacy paradox: Small money, small costs, small talk. National Bureau of Economic Research Working Paper, No. 23488. Available at http://www.nber.org/papers/w23488 (Accessed: July 13, 2018).

Avgerou, C., & Madon, S. (2005). Information society and the digital divide problem in developing countries. In Perspectives and Policies on ICT in Society: An IFIP Tc9 (Computers and Society) Handbook, J. Berleur and C. Avgerou (eds.). Boston, MA: Springer US, 205-217.

Beaudouin-Lafon, M. (2004). Designing interaction, not interfaces. *AVI '04. Proceedings of the Working Conference on Advanced Visual Interfaces* (pp. 15–22). .

Beke, F. T., Eggers, F., & Verhoef, P. C. (2018). Consumer informational privacy: Current knowledge and research directions. *Foundations and Trends in Marketing, 11*(1), 1–71.

Bhattacharya, C. B., Korschun, D., & Sen, S. (2009). Strengthening stakeholder–company relationships through mutually beneficial corporate social responsibility initiatives. *Journal of Business Ethics, 85*(2), 257–272.

Blevis, E. (2007). Sustainable interaction design: Invention & disposal, renewal & reuse. *SIGCHI Conference on Human Factors in Computing Systems,* 503–512.

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

Brey, P. A. E. (2012). Anticipating ethical issue in emerging IT. *Ethics and Information Technology, 14*(4), 305–317.

Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies* (1st ed). New York: W.W. Norton & Company.

Brynjolfsson, E., & McAfee, A. (2017). *Machine, platform, crowd: Harnessing our digital future.* New York: W. W. Norton & Company, USA.

Bynum, T. W. (2001). Computer ethics: Its birth and its future. *Ethics and Information Technology, 3*(2), 109–112.

Chahal, H., & Sharma, R. D. (2006). Implications of corporate social responsibility on marketing performance: A conceptual framework. *Journal of Services Research, 6*(1), 205–216.

Chatterjee, S., Moody, G., Lowry, P. B., Chakraborty, S., & Hardin, A. (2015). Strategic relevance of organizational virtues enabled by information technology in organizational innovation. *Journal of Management Information Systems, 32*(3), 158–196.

Chatterjee, S., Sarker, S., & Fuller, M. A. (2009). A deontological approach to designing ethical collaboration. *Journal of the Association for Information Systems, 10*(3), 138–169.

CNN (2013). Target: 40 million credit cards compromised. Available at https://money.cnn.com/2013/12/18/news/companies/target-credit-card/index.html (Accessed: July 8, 2019).

Council of the European Union (2016). General Data Protection Regulation. Available at http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf (Accessed: July 13, 2018).

Crawford, K., & Calo, R. (2016). There is a blind spot in AI research. Nature, October 13, Available at https://www.nature.com/news/there-is-a-blind-spot-in-ai-research-1.20805 (Accessed: July 14, 2018).

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342.

Culnan, M. J., & Williams, C. C. (2009). How can ethics enhance organizational privacy: Lessons learned from the ChoicePoint and TJX data breaches. *MIS Quarterly, 33*(4), 673–687.

D'Adderio, L. (2011). Artifacts at the centre of routines: Performing the material turn in routines theory. *Journal of Institutional Economics, 7*(2), 197–230.
Dance, G.J.X., LaForgia, M., & Confessore, N. (2018). As Facebook raised a privacy wall, it carved an opening for tech giants. The New York Times, Available at https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html (Accessed: March 18, 2019).
Deshpandé, R., & Webster, F. E. (1989). Organizational culture and marketing: Defining the research agenda. *Journal of Marketing, 53*(1), 3–15.
Diefenbach, S., & Ullrich, D. (2018). *Disrespectful technologies. Social norm conflicts in digital worlds. 9th International Conference on Applied Human Factors and Ergonomics, Orlando, Florida, USA*.
Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research commentary—informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. *Information Systems Research, 26*(4), 639–655.
Feldman, D. C. (1984). The development and enforcement of group norms. *The Academy of Management Review, 9*(1), 47–53.
Finkelstein, S., & Hambrick, D. C. (1990). Top-management team tenure and organizational outcomes: The moderating role of managerial discretion. *Administrative Science Quarterly, 35*(3), 484–503.
Floridi, L. (2010). Ethics after the information revolution. In L. Floridi (Ed.). *Cambridge Handbook of Information and Computer Ethics* (pp. 3–19). Cambridge: Cambridge University Press.
FTC (2012). Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policy makers. Available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (Accessed: July 13, 2018).
Ghose, A. (2017). *Tap: Unlocking the mobile economy*. Cambridge, MA: MIT Press.
Godos-Díez, J.-L., Fernández-Gago, R., & Martínez-Campillo, A. (2011). How important are CEOs to CSR practices? An analysis of the mediating effect of the perceived role of ethics and social responsibility. *Journal of Business Ethics, 98*(4), 531–548.
Granville, K. (2018). Facebook and Cambridge Analytica: What you need to know as fallout widens. The New York Times, Available at https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html (Accessed: July 8, 2019).
Greenaway, K. E., Chan, Y. E., & Crossler, R. E. (2015). Firm information privacy orientation: A conceptual framework. *Information Systems Journal, 25*(6), 579–606.
Hadasch, F., Li, Y., & Mueller, B. (2013). IS security policy enforcement with technological agents: A field experiment. 21. European Conference on Information Systems (ECIS 2013), Utrecht, The Netherlands.
Hinds, P. J., Roberts, T. L., & Jones, H. (2004). Whose job is it anyway? A study of human-robot interaction in a collaborative task. *Human-Computer Interaction, 19*(1–2), 151–181.
Holtrop, N., Wieringa, J. E., Gijsenberg, M. J., & Verhoef, P. C. (2017). No future without the past? Predicting churn in the face of customer privacy. *International Journal of Research in Marketing, 34*(1), 154–172.
Homburg, C., & Pflesser, C. (2000). A multiple-layer model of market-oriented organizational culture: Measurement issues and performance outcomes. *Journal of Marketing Research, 37*(4), 449–462.
Homburg, C., Stierl, M., & Bornemann, T. (2013). Corporate social responsibility in business-to-business markets: How organizational customers account for supplier corporate social responsibility engagement. *Journal of Marketing, 77*(6), 54–72.
Hoppner, J. J., & Vadakkepatt, G. G. (2019). Examining moral authority in the marketplace: A conceptualization and framework. *Journal of Business Research, 95*(2), 417–427.
Inman, J. J., & Nikolova, H. (2017). Shopper-facing retail technology: A retailer adoption decision framework incorporating shopper attitudes and privacy concerns. *Journal of Retailing, 93*(1), 7–28.
Ihde, D. (1990). Technology and the lifeworld: From garden to earth. Bloomington, In: Indiana University Press.
Intezari, A., Taskin, N., & Pauleen, D. J. (2017). Looking beyond knowledge sharing: An integrative approach to knowledge management culture. *Journal of Knowledge Management, 21*(2), 492–515.
Isaac, M. & Mele, C. (2017). Video of killing casts Facebook in harsh light. The New York Times, April 18, A1.
ISO/IEC (2013). Information technology – Security techniques – Information security management systems – Requirements. American National Standards Institute.
John, L. K., Acquisti, A., & Loewenstein, G. (2010). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research, 37*(5), 858–873.
Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607–635.
Klopfer, P. H., & Rubenstein, D. I. (1977). The concept privacy and its biological basis. *Journal of Social Issues, 33*(3), 52–65.
Koerner, B.I. (2016). Inside the cyberattack that shocked the US government. Wired, Oct 23, 2016, Available at https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ (Accessed: July 8, 2019).
Lameijer, C.S., Mueller, B., & Hage, M.L. (2017). Towards rethinking the digital divide – Recognizing shades of grey in older adults' digital inclusion. 38. International Conference on Information Systems (ICIS 2017), Seoul, South Korea.
Lee, D.-J., Ahn, J.-H., & Bang, Y. (2011). Managing consumer privacy in personalization: A strategic analysis of privacy protection. *MIS Quarterly, 35*(2), 423–444.
Lee, J. E. R., & Nass, C. I. (2010). Trust in computers: The computers-are-social-actors (CASA) paradigm and trustworthiness perception in human-computer communication. In D. Latusek, & A. Gerbasi (Eds.). *Trust and Technology in a Ubiquitous Modern Environment: Theoretical and Methodological Perspectives* (pp. 1–15). IGI Global: Hershey, PA.
Lohr, S. (2018). Facial recognition works best if you're a white guy. The New York Times, February 12, B1.
Lwin, M., Wirtz, J., & Stanaland, A. J. S. (2016). The privacy dyad: Antecedents of promotion- and prevention-focused online privacy behaviors and the mediating role of trust and privacy concern. *Internet Research, 26*(4), 919–941.
Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power-responsibility equilibrium perspective. *Journal of the Academy of Marketing Science, 35*(4), 572–585.
Maignan, I., & Ferrell, O. C. (2004). Corporate social responsibility and marketing: An integrative framework. *Journal of the Academy of Marketing Science, 32*(1), 3–19.
Maignan, I., Ferrell, O. C., & Ferrell, L. (2005). A stakeholder model for implementing social responsibility in marketing. *European Journal of Marketing, 39*(9/10), 956–977.
Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355.
Marshall, K. P. (1999). Has technology introduced new ethical problems? *Journal of Business Ethics, 19*(1), 81–90.
Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36–58.
Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 45*(2), 135–155.
Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly, 10*(1), 5–12.
McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the. Information Society, 4*(3), 543–568.
Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35–57.
Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15–29.
Mingers, J., & Walsham, G. (2010). Toward ethical information systems: The contribution of discourse ethics. *MIS Quarterly, 34*(4), 833–854.
Montag, C., & Diefenbach, S. (2018). Towards homo digitalis: Important research issues for psychology and the neurosciences at the dawn of the internet of things and the digital society. *Sustainability, 10*(2), 415.
Moon, Y., & Nass, C. (1998). Are computers scapegoats? Attributions of responsibility in human–computer interaction. *International Journal of Human-Computer Studies, 49*(1), 79–94.
Moor, J. H. (1985). What IS computer ethics? *Metaphilosophy, 16*(4), 266–275.
Moor, J. H. (2006). The nature, importance, and difficulty of machine ethics. *IEEE Intelligent Systems, 21*(4), 18–21.
Moore, B. (1984). *Privacy: Studies in social and cultural history*. Armonk, NY: M.E. Sharpe.
Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics, 38*(8), 114–117.
Moriarty, J. (2016). Business ethics. Stanford Encyclopedia of Philosophy, Available at https://plato.stanford.edu/entries/ethics-business/ (Accessed: July 15, 2017).
Murali, V., Qi, L., Chaudhuri, S., & Jermaine, C. (2018). Neural sketch learning for conditional program generation. 6. International Conference on Learning Representations (ICLR 2018), Vancouver, Canada.
Nambisan, S., Lyytinen, K., Majchrzak, A., & Song, M. (2017). Digital innovation management: Reinventing innovation management research in a digital world. *MIS Quarterly, 41*(1), 223–238.
Olerup, A. (1989). Socio-technical design of computer-assisted work: A discussion of the ethics and Tavistock approaches. *Scandinavian Journal of Information Systems, 1*, 43–71.
Oz, E. (1992). Ethical standards for information systems professionals: A case for a unified code. *MIS Quarterly, 16*(4), 423–433.
Pentland, B. T., & Feldman, M. S. (2005). Organizational routines as a unit of analysis. *Industrial and Corporate Change, 14*(5), 793–815.
Porter, M. E., & Kramer, M. R. (2006). Strategy & society: The link between competitive advantage and corporate social responsibility. *Harvard Business Review, 84*(12), 78–92.
Rainie, L., & Zickuhr, K. (2015). Americans' views on mobile etiquette. Pew Research Center, Available at http://www.pewinternet.org/2015/08/26/americans-views-on-mobile-etiquette/ (Accessed: July 14, 2018).
Richter, A., & Riemer, K. (2013). Malleable end-user software. *Business & Information Systems Engineering, 5*(3), 195–197.
Robinette, P. Li, W., Allen, R. Howard, A.M., & Wagner, A.R. (2016). Overtrust of robots in emergency evacuation scenarios. 2016 11th ACM/IEEE International Conference on Human-Robot Interaction (HRI), 101–108.
Saeidi, S. P., Sofian, S., Saeidi, P., Saeidi, S. P., & Saaeidi, S. A. (2015). How does corporate social responsibility contribute to firm financial performance? The mediating role of competitive advantage, reputation, and customer satisfaction. *Journal of Business Research, 68*(2), 341–350.
Salam, M. & Stack, L. (2018). Do video games lead to mass shootings? Researchers say no. The New York Times, Available at https://www.nytimes.com/2018/02/23/us/politics/trump-video-games-shootings.html (Accessed: March 19, 2019).
Sarathy, R., & Robertson, C. J. (2003). Strategic and ethical considerations in managing digital privacy. *Journal of Business Ethics, 46*(2), 111–126.
Schein, E. H. (2004). *Organizational culture and leadership* (3d ed). San Francisco: Jossey-Bass.
Scholz, R. W., Bartelsman, E. J., Diefenbach, S., Franke, L., Grunwald, A., Helbing, D., et al. (2018). Unintended side effects of the digital transition: European scientists' messages from a proposition-based expert round table. *Sustainability, 10*(6).
Schumann, J. H., Von Wangenheim, F., & Groene, N. (2014). Targeted online advertising:

Using reciprocity appeals to increase acceptance among users of free web services. *Journal of Marketing, 78*(1), 59–75.
Schwartz, M., & Carroll, A. B. (2003). Corporate social responsibility: A three domain approach. *Business Ethics Quarterly, 13*(4), 503–530.
Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1016.
Solove, D. J. (2005). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564.
Soltani, A. (2019). Abusability testing: Considering the ways your technology might be used for harm. Enigma 2019. Burlingame, CA, USA.
Son, J. Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly, 32*(3), 503–529.
Stahl, B. C., Eden, G., Jirotka, M., & Coeckelbergh, M. (2014). From computer ethics to responsible research and innovation in ICT: The transition of reference discourses informing ethics-related research in information systems. *Information & Management, 51*(6), 810–818.
Stanaland, A. J. S., Lwin, M. O., & Murphy, P. E. (2011). Consumer perceptions of the antecedents and consequences of corporate social responsibility. *Journal of Business Ethics, 102*(1), 47–55.
Steenkamp, J.-B. E. M., & Geyskens, I. (2006). How country characteristics affect the perceived value of web sites. *Journal of Marketing, 70*(3), 136–150.
Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management, 8*(3), 349–411.
The Economist (2017). The big data breach suffered by Equifax has alarming implications. September 16, Available at https://www.economist.com/finance-and-economics/2017/09/16/the-big-data-breach-suffered-by-equifax-has-alarming-implications (Accessed: July 9, 2019).
Treviño, L. K., Weaver, G. R., & Reynolds, S. J. (2006). Behavioral ethics in organizations: A review. *Journal of Management, 32*(6), 951–990.
Tucker, C. E. (2012). The economics of advertising and privacy. *International Journal of Industrial organization, 30*(3), 326–329.
Ullrich, D., & Diefenbach, S. (2017). Truly social robots. Understanding human-robot interaction from the perspective of social psychology. Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2017), 39–45.
Ullrich, D., Butz, A., & Diefenbach, S. (2018). Who do you follow?: Social robots' impact on human judgment. HRI '18 Companion of the 2018 ACM/IEEE International Conference on Human-Robot Interaction, 265–266.
Van den Hoven, J., Doorn, N., Swierstra, T., Koops, B.-J., & Romijn, H. (eds.). (2014). Responsible Innovation 1 - Innovative Solutions for Global Issues. Dordrecht, the Netherlands, et al.: Springer.
Van den Hoven, J., & Lokhorst, G.-J. (2002). Deontic logic and computer-supported computer ethics. *Metaphilosophy, 33*(3), 376–386.
Van Doorn, J., Mende, M., Noble, S. M., Hulland, J., Ostrom, A. L., Grewal, D., et al. (2017). Domo Arigato Mr. Roboto: Emergence of automated social presence in organizational frontlines and customers' service experiences. *Journal of Service Research, 20*(1), 43–58.
Van Wynsberghe, A., & Robbins, S. (2018). Critiquing the reasons for making artificial moral agents. *Science and Engineering Ethics, 25*(3), 719–735.
Verbeek, P. P., & Kockelkoren, P. (1998). The things that matter. *Design. Issues, 14*(3), 28–42.
Versteeg, M.J.J.M. (2013). Ethics & gamification design: a moral framework for taking responsibility. Thesis, Faculty of Humanities.
Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146–1151.
Wade, M.R. (2017). The Digital Vortex in 2017: It's Not a Question of "When". Available at https://www.imd.org/research-knowledge/articles/digital-vortex-in-2017 (Accessed: May 17, 2019).
Walsham, G. (1996). Ethical theory, codes of ethics and IS practice. *Information Systems Journal, 6*(1), 69–81.
White, T., Zahay, D., Thorbjornsen, H., & Shavitt, S. (2008). Getting too personal: Reactance to highly personalized email solicitations. *Marketing Letters, 19*(1), 39–50.
Wieringa, J., Kannan, P. K., Ma, X., Reutterer, T., Risselada, H., Roodbergen, K. J., et al. (2019). Data analytics in a privacy-concerned world. *Journal of Business Research* forthcoming.
Wirtz, J., & Lwin, M. O. (2009). Regulatory focus theory, trust and privacy concern. *Journal of Service Research, 12*(2), 190–207.
Wirtz, J., Patterson, P., Kunz, W., Gruber, T., Lu, V. N., Paluch, S., et al. (2018). Brave new world: Service robots in the frontline. *Journal of Service Management, 29*(5), 907–931.
Wirtz, J., So, K. K. F., Mody, M., Chun, E. H., Liu, S., & Chun, H. (2019). Platforms in the peer-to-peer sharing economy. *Journal of Service Management, 30*(4), 452–483.
Wolfangel, E. (2017). Google und die Frau am Herd. *die ZEIT,* 35.
Wright, D. (2011). A framework for the ethical impact assessment of information technology. *Ethics and Information Technology, 13*(3), 199–226.
Xie, E., Teo, H.-H., & Wan, W. (2006). Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. *Marketing Letters, 17*(1), 61–74.
Yang, Xiaohua, & Rivers, Cherly (2009). Antecedents of CSR practices in MNCs' subsidiaries: A stakeholder and institutional perspective. *Journal of Business Ethics, 86*(2), 155–169.