CORPORATE DIGITAL RESPONSIBILITY – EXTENDED CONCEPTUALIZATION AND EMPIRICAL ASSESSMENT

Cristina A. Mihale-Wilson  
*Goethe University Frankfurt*, mihale-wilson@wiwi.uni-frankfurt.de

Jan Zibuschka  
*Robert Bosch GmbH*, jan.zibuschka@de.bosch.com

K. Valerie Carl  
*Goethe University Frankfurt*, kcarl@wiwi.uni-frankfurt.de

Oliver Hinz  
*Goethe University Frankfurt*, ohinz@wiwi.uni-frankfurt.de

Follow this and additional works at: [https://aisel.aisnet.org/ecis2021_rp](https://aisel.aisnet.org/ecis2021_rp)

**Recommended Citation**

[https://aisel.aisnet.org/ecis2021_rp/80](https://aisel.aisnet.org/ecis2021_rp/80)

This material is brought to you by the ECIS 2021 Proceedings at AIS Electronic Library (AISeL). It has been accepted for inclusion in ECIS 2021 Research Papers by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
CORPORATE DIGITAL RESPONSIBILITY – EXTENDED CONCEPTUALIZATION AND EMPIRICAL ASSESSMENT

Research Paper

Cristina A. Mihale-Wilson, Goethe University Frankfurt, Frankfurt am Main, Germany, mihale-wilson@wiwi.uni-frankfurt.de
Dr. Jan Zibuschka, Robert Bosch GmbH, Renningen, Germany, Jan.Zibuschka@de.bosch.com
K. Valerie Carl, Goethe University Frankfurt, Frankfurt am Main, Germany, kcarl@wiwi.uni-frankfurt.de
Prof. Dr. Oliver Hinz, Goethe University Frankfurt, Frankfurt am Main, Germany, ohinz@wiwi.uni-frankfurt.de

Abstract
The digital economy holds new chances for value creation but also risks for both companies and customers alike. Within this context, the Corporate Digital Responsibility (CDR) movement gains traction. Building on the well-established Corporate Social Responsibility paradigm, CDR entails a set of rules through which it seeks to ensure an ethical and responsible development, deployment, and use of digital technologies. To date, the scholarly conceptualization of CDR is still in its infancy. This study pursues two main objectives: Firstly, this study seeks to contribute to CDR theory by providing a more in-depth conceptualization of the concept. Secondly, this study provides guidance for the implementation of CDR in practice, based on an empirical foundation. To this end, we conduct a series of Best-Worst Scaling studies with 515 German-speaking participants and examine consumers’ perspectives on various ethical guidelines from CDR.

Keywords: corporate digital responsibility, ethical guidelines, consumer perspective.

1 Introduction
Advancements in digital technologies allow for the development of more sophisticated and efficient digital products and services. Nevertheless, besides all the new opportunities for value creation, digitalization also holds a range of risks and challenges (Hess et al., 2016; Thorun et al., 2017) that managers need to cope with. In an attempt to harness the advantages of digitalization by adequately addressing its associated challenges, we can observe the emergence of a Corporate Digital Responsibility (CDR) debate.

At its core, CDR is closely related to and has similar goals like the concept of Corporate Social Responsibility (CSR). While CSR aims to minimize the negative impacts and maximize the positive impacts of corporate practices on socially and environmentally relevant issues (Maignan and Ralston, 2002), CDR intends to minimize the adverse effects of digitalization while maximizing the positive impacts of corporate digital activities. In this vein, CDR seeks to ensure an ethical and responsible development, deployment, and use of digital technologies and data.

To date, the CDR debate is strongly driven by practitioners and other policy-related initiatives, as its scholarly conceptualization is still in its infancy (Lobschat et al., 2021) albeit digitalization already
brought up unprecedented challenges (e.g., Nambisan et al., 2017). Recently, numerous initiatives evolved around the CDR idea or widened their focus concerning this topic. Supranational organizations like the European Union, the OECD or the UN are developing guidelines, laws (e.g., EU General Data Protection Regulation (GDPR), 'European Business Network for Corporate Social Responsibility', 'OECD Guidelines for Multinational Enterprises', 'UN Sustainable Development Goals', 'UN Global Compact') or working groups which try to establish CDR in the corporate mindset. Additionally, we can also see national and industry-led initiatives (e.g., the German 'Corporate Digital Responsibility Initiative') where industry leaders want to set a good example by committing to ethical business practices in the digital world. Within this debate, experts have formulated eight CDR norms as a basis for ethical and responsible digital business practices.

Aiming to advance the scholarly debate on CDR, this study pursues two main objectives: Firstly, as a theoretical contribution, this study seeks to contribute to the emerging knowledge about CDR. To this end, we demonstrate that not only is CDR an extension of CSR (Matten and Moon, 2008) in the digital context, but its norms, i.e. the ones identified by Thorun et al. (2017), address significant new challenges, motivating research on it as a distinct topic. Building on an initial empirical ranking of the existing CDR norms, we offer a deeper conceptualization of the most significant subfields of CDR, which we also rank. In this, we also address the issue that existing conceptualizations of CDR have not been explored in an empirical, quantitative fashion.

Secondly, there are currently few concrete recommendations on how CDR could be implemented. This work seeks to close this theoretical gap, while at the same time contributing to the implementation of CDR in practice: The implementation of CDR norms and practices can be pursued in many ways and at various levels (Matten and Moon, 2008). As resources to be spent on CSR and CDR are limited, a successful CDR implementation hinges on companies’ ability to pursue CDR norms and measures at levels that are important for key stakeholders involved (Kesavan et al., 2013).

In this work, we focus on consumers as one key stakeholder group and conduct a series of studies with 515 German-speaking participants to derive insights about which CDR norms, practices, and manifestations consumers value most. This way, we empirically validate the discriminatory power of existing conceptualizations of CDR and offer a more in-depth analysis of the most relevant norms.

2 Theoretical Background

As mentioned previously, the Corporate Digital Responsibility (CDR) concept is closely related to the concept of Corporate Social Responsibility (CSR). Nevertheless, CDR merits scholarly attention on its own, as it accommodates the digital world's peculiar challenges (Lobschat et al., 2021). To delineate the differences between CSR and CDR, we first discuss CSR's key ideas and elements. Then, by drawing on existing literature on the unique ethical and social challenges that the digital context presents, we discuss CDR's core components.

2.1 Corporate Social Responsibility

According to one of the most widely accepted definitions of CSR (Pirsch et al., 2007), the concept consists of economic, legal, ethical, and discretionary (philanthropic) expectations that society has of organizations (Carroll, 1979). These expectations translate into company responsibilities, which sets the frame of business-society relations (Matten and Moon, 2007). Economic responsibilities relate to companies’ primary aim to generate profits and serve their stakeholders while being sustainable in the long term. The legal responsibilities relate to regulations, and laws companies must comply with. One such legal responsibility is, for instance, that companies provide products that meet the minimal legal requirements. The ethical responsibility refers to companies’ obligations to do “what is right, just and fair, even when they are not obliged to by the legal framework” (Matten and Moon, 2007, p. 337), while the companies’ philanthropic responsibilities refer to various activities aimed at promoting the welfare of the communities to which they have ties to. Notably, companies’ economic and legal responsibilities are necessary conditions for companies to survive. In contrast, companies’ ethical and
philanthropic responsibilities are only desirable (Matten and Moon, 2007). Even so, based on the idea that companies can, in the short term, decide on the extent of addressing specific responsibilities, the CSR concept envisions that companies pursue activities and initiatives that go beyond the necessary conditions to be able to conduct business. In this sense, companies can, for instance, decide to surpass their economic responsibilities towards their suppliers and employees while meeting only their minimum responsibilities towards their shareholders. Pursuant its goals to meet companies' economic, legal, ethical, and philanthropic responsibilities, CSR strategies can include a variety of activities related to the environment, product safety, human rights, human dignity, alleviating global poverty, eradicating pandemic diseases, economic development, sustainability, community involvement and many more (Kesavan et al., 2013).

2.2 Corporate Digital Responsibility

Although CSR and CDR share common values, norms, and an organization’s commitment towards ecological and social challenges at large, CDR should be considered separately from CSR. CDR addresses challenges to organizations’ ethical behavior that are unique to the digital world and go far beyond CSR. Especially, “exponential growth in technological development, malleability of technologies and data in use, and pervasiveness of technology and data” (Lobschat et al., 2021, p. 876) manifest particularities of digital technologies. Thus, CDR and CSR represent complementary but also sometimes overlapping concepts of business ethics. Compared to CSR, CDR addressed the unprecedented challenges related to the digital world. In this respect, prior work on ethical and social issues of digitalization suggests that digital technologies such as the Internet of Things, digital platforms, robotics, artificial intelligence, augmented reality, and social media induce six central societal and ethical challenges for privacy, autonomy, security, human dignity, justice, and balance of power (Royakkers et al., 2018).

Privacy challenges relate to companies' and consumers' conflicting interests when collecting and processing consumer data (Royakkers et al., 2018). While companies see data as a critical production factor for value creation and wish to collect as much data as possible, consumers would like to control their data and wish to protect it (Awad and Krishnan, 2006). Besides, as digital products and services are growing more sophisticated to fit customers' needs better, consumers call for more transparency on where and how their data is used. As interconnected intelligent devices continually gather, process, and exchange data about their usage and usage context, it becomes increasingly complicated to track and understand data flows and how data is processed (Royakkers et al., 2018).

Autonomy challenges relate to digital technologies’ ability to take action without the interference of their user. Because fully automated artificial intelligence-enabled systems or robots can, for instance, make decisions or perform actions without human involvement and permission of their user, scholars raise the question whether and under which circumstances it would be ethical for humans to stay out of the loop of the decision making of such systems (Goodall, 2014). Additionally, digitization also creates a series of safety challenges, as it enables new types of criminal activities. While data and identity theft are present in everybody's minds, digital technologies also gave rise to cyber-terrorism that targets individuals' possessions and their physical and mental health (Gross et al., 2016).

Balance of power issues represent another critical challenge of digitization. As digital technologies enable companies to operate globally and scale their businesses quickly and at low cost (Royakkers et al., 2018), digital markets suffer from "winner takes it all" dynamics that allow various digital platforms to develop monopolistic positions. These monopolistic positions can then harm consumers' economic interests and promote discrimination and unfair competition (Scholz, 2016).

Finally, digital technologies are also linked to human dignity and justice challenges. While human dignity challenges refer to digital technologies' potential to exacerbate existing digital divides, justice challenges relate to their potential to promote discrimination, digital exclusion, and wrongful stigmatization (Royakkers et al., 2018). Digital divides refer to the inequalities arising when individuals, social groups, or regions do not have access or the skills necessary to harness digital
technologies (Wei et al., 2011). Due to the ubiquity of digitization in everyday personal and professional life, the accessibility of technology and digital products and services becomes a matter of social inclusion (Hess et al., 2016; Newell et al., 2006; Thorun et al., 2017). In this sense, individuals with improper access to technology or digital products and services will be disadvantaged in various ways (Hsieh et al., 2008; Lameijer et al., 2017). In addition to the importance of technology access, participation in the digital economy also requires suitable sets of skills—i.e., technology literacy. As digital technologies enable the automation of various occupations and thus reduce the overall number of jobs available, they likely promote discrimination and unjust exclusion (Royakkers et al., 2018).

Together, these challenges indicate that social responsibility within the digital context receives an extended connotation that requires that CDR and CSR are conceptualized separately. To date, the scholarly conceptualization of CDR is still in its infancy (Lobschat et al., 2021). The current CDR-related debate is strongly driven by practitioners and other policy related initiatives. Within this practice-driven debate (Thorun et al., 2017; United Nations, 2016), experts articulated eight norms suitable to promote ethical and responsible management and use of technology and data (see Table 1). Although these norms were articulated within the practice-driven debate, prior Information Systems and Business Ethics literature corroborate their theoretical validity.

Table 1 presents the CDR norms proposed by practice and indicates exemplary related literature. The proposed norms address potentially negative impacts of digitization and associated challenges. Thus, Table 1 theorizes the link between the proposed CDR norms and the addressed digitization challenges discussed above, indicating the expediency of the proposed CDR norms. We use the remainder of this section to briefly present the individual CDR norms and the scholarly literature related to them.

<table>
<thead>
<tr>
<th>CDR norm (Thorun et al., 2017)</th>
<th>Norm description (based on Thorun et al., 2017)</th>
<th>Exemplary related work</th>
<th>Challenges addressed (Royakkers et al., 2018)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Access</td>
<td>Consumers should have access to basic digital goods and services.</td>
<td>Hsieh et al. (2008); Lameijer et al. (2017); Venkatesh and Sykes (2013)</td>
<td>Justice</td>
</tr>
<tr>
<td>II. Education and awareness</td>
<td>Consumers should be educated. This includes their awareness of ecological, social, and societal aspects and the economic consequences of their consumption decisions.</td>
<td>Awad and Krishnan (2006); Granados et al. (2010)</td>
<td>Human dignity</td>
</tr>
<tr>
<td>III. Information and transparency</td>
<td>Consumers should have access to appropriate information so that they can be informed according to their individual wishes and needs.</td>
<td>Bourreau et al. (2015); Hinz et al. (2011)</td>
<td>Privacy, Autonomy</td>
</tr>
<tr>
<td>IV. Economic interests</td>
<td>The economic interests of consumers should be protected and promoted.</td>
<td>Daughety and Reinganum (1995); Smith (2017)</td>
<td>Balance of power</td>
</tr>
<tr>
<td>V. Product safety and liability</td>
<td>Consumers should be protected from risks to their health and safety.</td>
<td>Bélanger and Crossler (2011); Gimpel et al. (2018); OECD (2017)</td>
<td>Security, Autonomy</td>
</tr>
<tr>
<td>VI. Privacy and data security</td>
<td>The protection of consumers' privacy and the free flow of information should be ensured, and both protected and secure payment mechanisms should be offered.</td>
<td>European Parliament (2016); Thorun et al. (2017)</td>
<td>Privacy</td>
</tr>
<tr>
<td>VII. Dispute resolution and awareness</td>
<td>Consumers should have access to effective dispute settlement and appeal procedures.</td>
<td>European Parliament (2016); Thorun et al. (2017)</td>
<td>Balance of power, Human dignity, Justice</td>
</tr>
<tr>
<td>VIII. Governance and participation mechanisms</td>
<td>Legal organizations and regulators should ensure that there are appropriate governance and participation mechanisms in place.</td>
<td>Lobschat et al. (2021); Thorun et al. (2017)</td>
<td>Balance of power, Justice</td>
</tr>
</tbody>
</table>

Table 1. CDR Norms that can serve as a (preliminary) conceptualization of CDR.
(I) Access adheres to the possibility of physically accessing technology and digital products or services (Hsieh et al., 2008; Lameijer et al., 2017). (II) Education and awareness entails all activities which enable consumers to retrieve information and advice, how to buy goods and services online (Thorun et al., 2017; United Nations, 2018), but also enabling individuals to understand which data is needed for online transactions; what are their rights regarding data security and privacy; and how they can make use of them. Additionally, this CDR norm also envisions that companies enable consumers to understand the implications of their digital consumption and behavior and make more informed technology and digitalization-related decisions in the future. Both CDR norms are closely related to the digital divides arising from disparities in technology access and skills. To date, the digital divide phenomenon was studied on numerous occasions and in various settings (e.g., Hsieh et al., 2008; Venkatesh and Sykes, 2013). Thus, we can currently draw on a rich body of literature on the topic. Independent of their research setting, prior literature on the digital divide unanimously concludes that disparities in technology access or technology-related skills have adverse effects on individuals and society. Against this background, it seems appropriate that an ethical, responsible, and sustainable approach to technology should include activities aimed at reducing disparities in technology access and technological literacy.

(III) Information and transparency: Besides education, another essential prerequisite for informed decisions is information and transparency. In general, along with the rise of the Internet, and instant access to information, consumers’ demand for information and transparency has also increased steadily (Awad and Krishnan, 2006; Granados et al., 2010). As consumers "expect to be very well informed, spoiled and empowered" (Granados and Gupta, 2013, p. 637), companies are pressured to be more transparent. Thereby, transparency is not only a matter of representing the features of a product or service explicitly. Instead, consumers’ demand for transparency touches on pricing, quality, products’ provenance, and the resources such products were made of (Granados and Gupta, 2013). This way, information transparency is increasingly viewed as a strategic decision affecting firms’ success (Awad and Krishnan, 2006; Granados and Gupta, 2013; Granados et al., 2010).

(IV) Consumers’ economic interests: Closely related to information transparency, the concept of CDR envisions that companies are also following consumers’ economic interests. The best way to ensure this is the issuance of appropriate competition policies (United Nations, 2018). The conflicting economic interests between companies and consumer in the context of digitalization has been studied for instance in the context of the net neutrality (e.g., Bourreau et al., 2015; Peitz and Schuettt, 2016), interoperability (e.g., Lewis, 2013) or price strategies (e.g., Hinz et al., 2011; Weisstein et al., 2013). Despite the different foci and the variety of research questions that existing studies investigate, the current body of literature suggests that protecting consumers' economic interests can pay off. In this sense, studies on the pricing of digital products and services show that increasing profits in the short term with price discrimination strategies (e.g., Elmaghraby and Keskinocak, 2003; Weisstein et al., 2013) can, in the long run, lead to consumer distrust and willingness to churn (e.g., Richards et al., 2016; Weisstein et al., 2013). Given the positive relationship between customer loyalty and customer profitability (Lars, 2007), transparency on companies' pricing policy might be a useful and rewarding strategy worth pursuing.

(V) Product safety and liability: Traditionally, the product safety of goods in the real world relates to the extent to which the operation and use of products are risky and can cause injuries. At the same time, liability refers to product or service suppliers’ actions in case of injury (Daughety and Reinganum, 1995). Notably, in the “biological” world, companies cannot limit their liability towards a customer in any way (Daughety and Reinganum, 1995), as most of the injuries can be traced back to their origin. However, in a digitalized world where products and services from different vendors are interconnected and continuously exchange and use data to provide personalized products and services, it may be far more challenging to find the undeniable source of injury and loss (Smith, 2017). Moreover, in the context of digital goods and services, consumers can suffer not only psychological but also mental injuries (Gross et al., 2016), complicating the safety and liability issue even further. Thus, the CDR concept encourages companies and policymakers to address the various facets of safety and liability for interconnected digital products and services.
(VI) **Data privacy and security:** To date, data privacy and security remain two of the significant concerns related to the adoption and use of information technologies (Mason, 1986). Hence, it is not surprising that data privacy and security have enjoyed considerable attention from policymakers and scholars alike (e.g., Bélanger and Crossler, 2011; Heimbach and Hinz, 2018). The topic is subject to regulations (e.g., EU General Data Protection Regulation (GDPR)), which define the minimum requirements of data privacy and security companies must comply with. While non-compliance with the minimum requirements can have negative legal and financial consequences (Goel and Shawky, 2009; OECD, 2017), compliance does not stand out positively. Against the background that companies can positively influence consumers’ perceptions through strategic initiatives (Hann et al., 2007), this CDR norm encourages companies to go beyond the currently valid privacy and security regulations.

(VII) **Dispute resolution and redress:** Motivated by the complications arising from interoperability and interconnectivity between products and services from various providers, the CDR concept also addresses the case of dispute resolution and redress. In general, dispute resolution refers to the mechanisms aiming to provide consumers who have suffered (economic) harm from transactions across borders, to solve their complaints and receive redress (Clifford and Van Der Sype, 2016). As digitalization enables companies to operate across borders, the CDR concept envisions uncomplicated, unified, and efficient dispute resolution and redress mechanisms for all consumers. More specifically, CDR suggests that consumers should have the option to place complaints easily and free of charge, while the processing of the complaints should be fast, fair, and transparent (European Parliament, 2016; Thorun et al., 2017).

(VIII) **Governance and participation mechanisms:** Ultimately, it is notable that CDR also acknowledges the need that governments continuously adjust regulations to "steer the digitalization process in the right direction" (Thorun et al., 2017, p. 91). In this sense, the CDR concept calls for appropriate governance and participation mechanisms (i.e., efficient law-making, regulatory conditions, and well-established enforcement) in a digitalized world. Indeed, we can already observe coupling between the CDR elements discussed above and the (legal) frameworks. The majority of CDR elements discussed above are currently anchored or partially represented in current (legal) frameworks of the European Union (i.e., the European Unions' GDPR) or the UN (i.e., the United Nations' Guidelines for Consumer Protection). However, besides the current state of regulation, CDR calls for continuous monitoring and adaptation of the current regulatory frameworks in accordance with new technological developments.

3 **Empirical Analysis on Consumers’ Valuation of CDR Norms and Implementations**

Similar to CSR, voluntariness is the core idea of CDR. Albeit various aspects of the mentioned CDR norms are already regulated—for instance by the GDPR—it is important to remember that CDR represents activities that companies can implement voluntarily and in addition to the minimum regulations that might apply. Accordingly, CDR activities incur additional costs and investments that companies need to account for. The costs and investments necessary to implement CDR norms depend on their implementation specification. That is, the implementation of CDR norms and practices can be done in many ways and at various levels (Matten and Moon, 2008). Due to the numerous possible implementations of CDR norms and companies' limited resources, it is beyond the majority of businesses' reach to implement all CDR norms at once. Under the premise that successful CDR implementation hinges on companies’ ability to pursue CDR norms and practices at levels that are important for key stakeholders (Kesavan et al., 2013), this work focuses on one important stakeholder group—consumers. Specifically, in this study, we elicit consumers’ preferences for various CDR norms.

Our empirical analysis follows a two-step approach: First, we empirically investigate which of the CDR norms formulated in the previous section are the most important for consumers. After identifying a ranking reflecting consumers’ perspective on the CDR norms presented, we conduct other empirical
studies to determine which of the implementation manifestations of the top three CDR norms consumers would desire most.

3.1 Method, Design, and Participants

To better understand consumers’ preferences for the proposed CDR norms and identify which CDR norms are worth implementing first, we conduct three Best-Worst Scaling (BWS) studies. Best-Worst Scaling is a well-established method to evaluate consumer preferences since decades (Auger et al., 2007; Hinz et al. 2015; Louviere et al. 2013). BWS is especially suitable for heterogeneous groups e.g., with regard to education or knowledge (Hinz et al., 2015), thus appropriate for the CDR context.

In general, BWS studies allow researchers to compare issues and people in a way that minimizes biases stemming from using scales or biases stemming from participants’ cultural backgrounds (Auger et al., 2007; Keller et al., 2021). As an enhanced version of paired comparisons (Auger et al., 2007; Cohen and Orme, 2004), BWS forces participants to repeatedly choose their most preferred and least preferred option from a varying set of options (Hinz et al., 2015; Kaufmann et al., 2018). BWS allows to compare more attributes than ranking methods also addressing the problem of assumed equal differences between two consecutive attributes (Bettman et al., 1990; Hinz et al., 2015). Additionally, the interpretation of choices is consistent across the whole sample.

The conducted BWS studies build on each others results and use the same participant sample. Our BWS studies were designed following Auger et al. (2007) and conducted with the online Dynamic Intelligent Survey Engine (DISE) implemented by Schlereth and Skiera (2012). Each BWS study consisted of seven choice sets from which participants could choose their most preferred and least preferred CDR-related attributes we wished to assess. Each prompted CDR attribute was presented supplemented by a brief description (e.g., see Table 1 for BWS study 1). To construct our choice sets, we used a Balanced Incomplete Block Design (BIBD) in which choice sets have to have the same number of items; each item occurs the same number of times across choice sets and equally often as any other item (Kaufmann et al., 2018). Figure 1 visualizes the main blocks of our first BWS study. The other two BWS studies were structured analogously and contained three building-blocks. The proposed CDR dimensions (see Table 1) cover a wide range of possible implementations.

As mentioned previously, all BWS studies in this manuscript build on each others results and use the same participant sample. A market research company provided a representative sample with 515 participants each answering all three BWS studies, also passing the attention and consistency checks. The sample has an almost equal gender split (45% females and 55% males) and is between 17 and 87 years old. While almost 25% of the participants were between 45 and 54 years old, 20% were between 35 and 44, another 20% between 65 and 74. In contrast, only 13% of respondents were between 17 and 34 years old. According to this age distribution, the majority of participants were employed full-time (47%), retired (26%), or employed part-time (17%). Notably, our sample’s education level approximates the education level across Germany well (for an overview of Germany’s education level, see Statistisches Bundesamt (2018)). Accordingly, most of the participants hold a secondary school diploma (35%), a high school diploma (21%), a Bachelors’ (8%), or a Master’s degree (22%). Only 14% of participants have a lower education status than secondary school certificate.

Figure 1. Study design – sections of the first BWS study.
3.2 BWS1: Consumers’ Valuation of the Proposed CDR Norms

In this first BWS experiment, we capture consumers’ valuation of the CDR norms presented in Table 1. Because our work focuses on companies and how companies should implement CDR, our BWS enquire all but the governance and participation mechanism element of CDR. The main rationale for excluding this element is that it lies predominantly in the hands of policymakers and other non-governmental regulatory organizations (Thorun et al. 2017). Since the governance and participation mechanism is out of the direct reach of companies it can be considered to be an exogenous force within a CDR framework.

Figure 2 shows a rank of the prompted CDR norms (in decreasing order from left to right), along with their averaged BW score, reflecting the relative importance of the choice sets across the entire participant sample, and the difference between the BW scores of the top three participant choices (Δ). It shows that across all participants, privacy and data security, along with product safety and liability, and information transparency are the CDR norms that have the highest valuation. In contrast, access, economic interests, and dispute resolution and redress are viewed by participants as the least problematic or pressing issues.

In detail, the graph in Figure 2 also suggests that CDR norms related to privacy and security and product safety and liability are of similar importance. In contrast, information transparency has lower importance than the former two. Further, although participants do not see access to digital products and services as problematic, they feel a further need for education and awareness. In this respect, the CDR norm related to education and awareness is twice as important (Δ=0.33) than the access. Consequently, we conclude that to date, consumer training, which increases the knowledge about digital products and services and the awareness of environmental, social, and societal issues and the economic consequences of consumption choices, is more important than access to digital products and services. Additionally, our results also show that participants do not think that their economic interests need to be protected or promoted. The majority of the participants (62.7%) rated this CDR norm as one of the three least important CDR norms; only 20% rated it as the most important. Altogether, the results in Figure 2 suggest that companies restricted in their CDR budget should first concentrate on the privacy and security and product safety and liability CDR dimensions. Once companies implemented these two CDR norms, they should implement more transparency as an additional key differentiator from competitors.

Expanding on our customer ranking of the key CDR norms, we conducted further empirical studies to determine which areas subsumed within the top ranked norms consumers would appreciate the most. Due to the complex, highly dynamic and nationally fragmented legal debate on product safety and liability of digital products and services (Desai, 2014; Howells et al., 2017) we could not identify stable safety and liability implementations that would form a solid basis for empirical assessment. Therefore, our further empirical investigation focuses on the privacy and security and information and transparency CDR norms, which were ranked first and third in our initial ranking.
3.3 BWS2: Consumers’ Valuation of Various Implementations of the Privacy and Security Norm

The importance of data privacy and security is a widely discussed research topic in information systems (e.g., Bélanger and Crossler, 2011; Hann et al., 2002). Amongst one of the undisputed major consumer concerns in the digital economy, information privacy refers, amongst others, to the consumer's capability to control their information stored and the handling of their data, including the monetization (Bélanger and Crossler, 2011; Goodwin, 1991). The topic of privacy is multifaceted and features various aspects. Smith et al. (1996), for instance, suggest that privacy has four main aspects: one aspect of privacy relates to data collection. The second aspect adheres to unauthorized secondary use of information for both organization-specific internal and other external purposes. Further, the third privacy aspect is improper access, while information accuracy (i.e., errors) represents a fourth important privacy aspect. In practice, these aspects reappear in data privacy and security regulations such as the GDPR or OECD Guidelines for Protection of Privacy and Transborder Flows of Personal Data. According to the OECD (2013) guidelines, for instance, privacy and data security should consider eight main principles: (1) data collection limitation; (2) data quality; (3) purpose specification; (4) use limitation; (5) security safeguards; (6) openness; (7) individual participation; (8) accountability principle. Akin, the GDPR, provides eleven privacy and security-relevant principles (Tesfay et al., 2018), similar to the OECD Guidelines. Based on scholarly work on data privacy and security and from the current state of legislation (i.e., GDPR, OECD Guidelines), we derived seven implementations of the data privacy and security CDR norm (see Table 2).

<table>
<thead>
<tr>
<th>Implementation</th>
<th>Description</th>
<th>Exemplary related work</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited / restricted data collection</td>
<td>The collection of (personal) data must be limited, lawful, and fair, usually with the knowledge and / or consent of the user.</td>
<td>GDPR; Smith et al. (1996); Thorun et al. (2017)</td>
</tr>
<tr>
<td>Clear purpose of data collection</td>
<td>The purpose of the data collection must be clearly stated at the time of collection.</td>
<td>Smith et al. (1996); Thorun et al. (2017)</td>
</tr>
<tr>
<td>Restricted data use</td>
<td>The use or disclosure of data must be limited to the previously agreed purpose(s) or only for closely related purposes.</td>
<td>GDPR; Smith et al. (1996); Thorun et al. (2017)</td>
</tr>
<tr>
<td>Openness about data processing practices</td>
<td>Businesses need to be transparent about their data processing practices.</td>
<td>European Parliament (2016); Thorun et al. (2017); Turilli and Floridi (2009)</td>
</tr>
<tr>
<td>Secure storage and processing of user data</td>
<td>The storage and processing of user data must be subject to appropriate security.</td>
<td>GDPR; Thorun et al. (2017)</td>
</tr>
<tr>
<td>Data quality</td>
<td>User data collected and stored by companies must be relevant, accurate, and up-to-date.</td>
<td>Martin (2015); Smith et al. (1996); Thorun et al. (2017)</td>
</tr>
<tr>
<td>Access and correction</td>
<td>Users must be able to view and correct the user data stored by companies.</td>
<td>GDPR; Martin (2015); Smith et al. (1996); Thorun et al. (2017)</td>
</tr>
</tbody>
</table>

Table 2. Overview of data privacy and security aspects prompted in BWS Study 2.

Figure 3 displays the averaged BW ratings of the individual CDR implementations prompted in the study. It shows that in terms of privacy and security aspects, secure storage and processing of data, a restricted data collection, and data access and correction are among the most important for participants. At the same time, consumers' report that openness about data processing practices and a clear purpose of data collection or data quality play a rather subordinate role.

The averaged BW scores of the various privacy and security implementations and the differences between the individual averaged scores indicate that participants view the secure storage and processing of data as the top-ranked norm (averaged BW score of 1.29). At the same time, participants rated access and correction (averaged BW score of 0.26) to be similarly important as restricted data use (averaged BW score of 0.22), but ranked it significantly lower than restricted data collection (which features an averaged BW score of 0.70). In short, we see a significantly higher ranking for
technological enforcement of security and privacy as opposed to mere documentation of the peculiarities, as is illustrated e.g. by the gap between restricted data collection and restricted data use. Consequently, companies should pay particular attention to implementing secure storage and processing of the data and restricted data collection. As security and restricted data collection are not readily observable for consumers, companies which wish to differentiate themselves on CDR might aim at a higher prioritization of access for consumers to data stored about them and/or restrict their data processing to use and disclosure to only previously agreed purposes. Under regimes already enforcing such functionality, such as the EU’s GDPR, companies aiming to differentiate might move down to the lower half of the ranking, aiming to differentiate on openness or data quality.

Figure 3. Averaged BW ratings of privacy and security implementations across participants.

3.4 BWS3: Consumers’ Valuation of Various Implementations of the Information and Transparency Norm

In contrast to the scholarly debate on the data privacy and security topic, research on transparency and its benefits is scarce and dispersed across various disciplines (Granados et al., 2010). Prior studies suggest that companies' transparency decisions involve trade-offs managers need to consider. While full transparency might lead to an optimal outcome in some cases (e.g., related to the performance of supply chains), it might have adverse or inappropriate consequences in other cases (Granados et al., 2010). Even though transparency decisions in the business context are not straightforward, scholars (e.g., Granados et al., 2010) postulate that there is much to be gained from adopting the right transparency strategy (in the right situation). This notion is also supported by our first BWS study results, which shows that consumers' rate information and transparency to be one of the top three valued CDR Norms.

Existing research related to information and transparency suggests that companies can pursue transparency at different strategic and operational levels: For one, companies can choose to disclose relevant information on products and services online. Furthermore, companies could choose to disclose information about their business models (i.e., the way they make profits) (Mihale-Wilson et al., 2019) or pricing strategies (e.g., Granados et al., 2010). Price discrimination policies, for instance, are enabled based on digital technologies that can continuously collect and process personal data (e.g., Acquisti and Varian, 2005; Hui et al., 2007). In this sense, companies can implement transparency by adequately informing (potential) consumers about privacy and data security practices, the collection, storage, or handling of personal data (European Parliament, 2016; Turilli and L. Floridi, 2009). Companies can also implement transparency without disclosing sensitive business data to the world using certifications—a widely adopted institution-based mechanism to increase consumers’ trust (Carl and Mihale-Wilson, 2020; Chang et al., 2013). Finally, currently applicable legislation (e.g., GDPR) and guidelines (e.g., UN Guidelines for Consumer Protection) suggest that companies should also provide transparent information on terms and conditions, final costs, goods, and services. Based on
related literature, the currently available regulations and suggestions made by the practice and government-driven debate on CDR (Thorun et al., 2017), the third BWS experiment prompts seven information and transparency-related implementations of CDR (see Table 3).

<table>
<thead>
<tr>
<th>Implementation</th>
<th>Description</th>
<th>Exemplary related work</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online information disclosure</td>
<td>Companies should provide complete and non-misleading information about their goods and services, terms and conditions, fees, and final costs.</td>
<td>Royakkers et al. (2018); Stohl et al. (2016); Thorun et al. (2017)</td>
</tr>
<tr>
<td>Adequate information on privacy policy</td>
<td>The company’s privacy policy should be written in easy-to-understand language, and presented simply (e.g., as a one-pager).</td>
<td>Royakkers et al. (2018); Thorun et al. (2017)</td>
</tr>
<tr>
<td>Certification</td>
<td>Business processes, products, and services should be certified, for example, concerning usability or data protection.</td>
<td>Chang et al. (2013); Yanisky-Ravid and Hallisey (2019)</td>
</tr>
<tr>
<td>Transparency on storage and processing</td>
<td>Transparency on storage and processing of personal data should be provided.</td>
<td>GDPR; Stohl et al. (2016); Thorun et al. (2017)</td>
</tr>
<tr>
<td>Transparency of data transmission</td>
<td>Companies should disclose whether they pass on the data of their users in any form to third parties.</td>
<td>European Parliament (2016); Turilli and Floridi (2009)</td>
</tr>
<tr>
<td>Transparency on data security incidents</td>
<td>Businesses should be required to report data security incidents (e.g., security breaches, data theft).</td>
<td>Thorun et al. (2017)</td>
</tr>
<tr>
<td>Transparency of the business models</td>
<td>Users should know how the company generates revenue with a product or service (for example, by selling additional features, advertising revenue, subscription fees).</td>
<td>Stohl et al. (2016); Mihale-Wilson et al. (2019)</td>
</tr>
</tbody>
</table>

Table 3. Overview of information and transparency implementations prompted in BWS Study 3.

Figure 4 visualizes participants’ choices in the BWS study and the differences in the averaged BW scores of the prompted transparency implementations. It shows that participants value transparency on data transmission, data security breaches, and storage and processing of data to be most important. Notably, the top three ranked implementations of transparency have relatively small differences between their averaged BW ratings (i.e., $\Delta=0.11$, $\Delta=0.08$). The same is true for the bottom three norms in the ranking. Between the two groups, online information disclosure sits as a single element of average ranking. It is notable that transparency of data transmission, storage and processing, as well as security breaches, is rated higher than the transparency of the company’s business terms, which may further underline the importance of the technological aspects of privacy and security in the context of CDR as opposed to documentation, as privacy policies and certification are seen as significantly less compulsory.

Figure 4. Averaged BW ratings of information and transparency implementations across participants.
4 Discussion and Conclusion

Aiming to advance the current state of research on CDR, this study had two main research objectives: Firstly, this work sought to contribute to CDR's scholarly conceptualization by sharpening it and putting it on an empirical foundation. This work’s second aim was to generate insights for CDR implementation. From a theoretical perspective, our study advances the conceptualization of the emerging concept of CDR by empirically showing that consumers' valuation of norms originating in the current practice-driven discourse varies significantly, offering a degree of validation for the current conceptualization of those norms (BWS1). Additionally, we sharpened the conceptualization of two of the three most relevant CDR norms, security and privacy and transparency, and also provide empirical results for those (BWS2&3). We also show how CDR norms address challenges specific to the digital economy, and thus merit investigation as an independent concept going beyond classical CSR.

Our results highlight the urgency for a (legal) framework regulating the product safety and liability issues unique to intangible and interoperable technology products and services. In contrast to the product safety and liability of tangible products, the liability regulations for digital products and services are still to be articulated. While scholars and regulators are currently not in agreement on how and whether intangible goods such as apps or software can fall under the currently available product regulations (Howells et al., 2017), our work shows the urgent need for action on this topic.

From a managerial perspective, our study presents concrete guidance for managers operating in the digital economy. Because implementing a CDR culture can be costly for organizations (Lobschat et al., 2021), this study attempts to support managers by presenting a concrete roadmap for how to start developing and implementing CDR norms into practice. Notably, a cost-benefit analysis of implementing a CDR culture in organizations was not the scope of this work. However, this work can serve as a basis for designing and conducting a study researching this essential managerial question.

Our analyses suggest that companies restricted in their CDR budget should first concentrate on implementing privacy and security, and product safety and liability CDR elements. In terms of privacy and security, companies should ensure that they implement state of the art security for storage and processing of personal information. Companies should, however, take into account that for the most advanced security technologies, customers' valuation does not keep up with the cost incurred (Mihale-Wilson et al., 2017), and we merely surveyed appropriate levels of security, not exceptionally high ones. Furthermore, our results reveal that customers also feel it is the companies' responsibility to restrict their data collection to what is needed for their purposes. Moreover, they also feel that it is relevant to access and correct the data collected and restrict the use of collected data—although these aspects are seen as significantly less relevant than restricted data collection.

Once companies implemented a sound set of actions serving the privacy and security, and product safety and liability dimensions, it is advisable to consider addressing CDR's information and transparency norm. In this regard, it is notable that participants rated transparency regarding data transmission, data security breaches, and storage and processing of data as the top 3 most desirable transparency implementations. While some companies (such as Google or the German Telekom) committed to more data transparency and allow their user to view and manage their data via online dashboards, proactive transparency on data security breaches is not observed. In terms of transparency of data breaches, it is notable that estimating the negative impact of privacy violations and security breaches is very challenging (Nofer et al., 2014). Hence, the effect of proactively coming forward on the number of breaches a company experienced is currently not well understood. Against this backdrop, companies considering to disclose sensitive information such as their business models or security attacks should do so only after carefully considering all potential effects of such action.

Despite our best efforts to ensure the reliability and validity of the results, it is essential to mention this study's limitations. One limitation relates to our sample, which consists of individuals living and working in Germany. For instance, participants rated the education and awareness element to be more important than access. This is not surprising when considering that our study was an online experiment where individuals already had to have access to digital products and services in order to participate. In general, the majority of the German population has access to the Internet and other digital products.
However, access to digital products and services might be a problem in other countries or for specific groups of people. Thus, testing our findings in the context of other countries could be a valuable future research path for advancing the CDR concept. Additionally, further testing should address possible regional biases due to media presence of certain CDR dimensions. Especially in the U.S. or Germany ‘privacy and data security’ is a frequently discussed topic in the media (Lobschat et al., 2021) and thus media presence might have an influence on customers’ assessment of the CDR concept. Furthermore, the evaluation of CDR might be influenced by the participants’ experience with digital technologies. For companies in Germany and the EU, it is notable that the only point with a positive BW rating that is not directly covered by the GDPR is working towards complete and non-misleading online information disclosure. Therefore, our study can also be seen as a strong validation of the European approach to privacy and data protection, with regulation covering those aspects that citizens most feel are part of corporations’ inherent responsibilities. That is not to say that CDR may not serve as a differentiator, as companies can implement those key aspects of the GDPR in an exemplary fashion.

Our examination of the CDR concept focused on customers as a key stakeholder group in the context of corporate responsibility. Notably, while consumers’ preferences for CDR implementations have been tested over various industries, companies might have a different focus in implementing CDR activities due to their industry affiliation, e.g. due to their dependence on necessary data processing. Thus, future research might evaluate customer preferences applied to different industries. However, the concept of CDR can also be applied to other stakeholder groups at the level of organizations or individuals facing comparable challenges in a digital world. Thus, we encourage further research to evaluate e.g., employees’ assessment of CDR preferences in their working environment or companies’ evaluation of the CDR concept in the business-to-business context (Lobschat et al., 2021).

Finally, it is noteworthy that due to its structure and research goal, this study ranks various CDR norms and guidelines from the consumers’ perspective but does not account for any consequences that the implementation of the various CDR norms or consumers’ valuation of those would have in practice, e.g. for groups strongly affected by lower ranking norms such as education or access. Hence, there is a need for further studies investigating and accurately calculating the final value of different CDR options for operationalization. After all, since companies can influence the consumer’s perception of a firm with its initiatives (Hann et al., 2007), an excellent implementation of various CDR norms has the potential to develop into a competitive advantage.

References


Twenty-Ninth European Conference on Information Systems (ECIS 2021), [Marrakesh, Morocco|A Virtual AIS Conference].


