Trust in open data applications through transparency

Christian Wiencierz
University of Münster, Germany

Marco Lünich
University of Düsseldorf, Germany

Abstract
Open data provide great potential for society, for example, in the field of smart cities, from which all citizens might profit. The trust of these citizens is important for the integration of various data, like sensitive user data, into an open data ecosystem. In the following study, we analyzed whether transparency about the application of open data promotes trust. Furthermore, we formulated guidelines on how to create transparency regarding open data in an ethical way. Using an open-data-based fictitious smart city app, we conducted an experiment analyzing to what extent communication of the technical open data application process and the ethical self-commitment for the transparent communication of data application affect trust in the app’s provider. The results indicate that the more information users obtain regarding the use of open data, the more trustworthy they perceive the app provider to be, and the more likely they are to use the app.

Keywords
Big data, ethics, open data, privacy concerns, smart cities, transparency, trust

Introduction
Open data have untapped potential that can benefit both individuals and society (Meijers et al., 2014). As an ideal of an open data ecosystem, a so-called “data commons,” in which big data become open data, is being discussed (World Economic Forum, 2012).

Corresponding author:
Christian Wiencierz, REACH – EUREGIO Start-up Center, University of Münster, Geiststraße 24-26, Münster 48151, Germany.
Email: christian.wiencierz@uni-muenster.de
Big data comprise high-volume, high-velocity, high-variety, and high-veracity information assets generated by using innovative and complex computer and storage systems in a way that makes these assets manageable and usable for organizations and persons (Scholz, 2017: 12–20; Wiencierz and Röttger, 2019). In this data commons, which is publicly accessible and free of charge, different big data streams from individuals and the public and private sectors are merged. Everyone can use, modify, and share these open data for any purpose. It is not traceable to a person and is compatible with applicable data protection laws in the respective country (Open Knowledge International, 2018a). The aim is “a world where knowledge creates power for the many, not the few” (Open Knowledge International, 2018b). The potential of open data for society becomes particularly obvious in the context of smart cities (Kitchin, 2014; Ojo et al., 2015). For example, big data in the form of citizens’ geo-tracking data, cities’ data from their traffic light systems, and car companies’ data from their vehicles can be saved as data commons. In turn, service providers can use these open data to develop an intelligent traffic management system. Although personal information is anonymized in the open data context, the risk of reidentification surfaces when sensitive, freely accessible data are combined with other data (De Montjoye et al., 2015). This potential risk of privacy infringement is significant and may evoke perceptions of ubiquitous surveillance (Zuboff, 2019).

If organizations want to establish the open data concept, they have to explain its potential and in particular they have to build trust in their open data applications (Martin and Murphy, 2017). Trust helps users to tolerate the vulnerability and risks they perceive in the context of open data (Harwood and Garry, 2017; McKnight et al., 2011). In this context, scientists and data privacy activists, among others, discuss the necessity for ethical principles and transparency in data applications in order to generate legitimacy and trust in the use of open data (Martin and Murphy, 2017; Meijers et al., 2014; Richterich, 2018). For instance, corresponding considerations have also accompanied recent debates concerning so-called tracing apps for battling the COVID-19 pandemic (Ada Lovelace Institute, 2020; Leins et al., 2020). Our research addresses the question of how differing degrees of transparency surrounding the generation and application of open data based on ethical principles influence stakeholders’ trust in the data-using organization.

Trust is built on cues which forms the trustees’ opinion in a trust relevant situation. Thus, trust essentially depends on the self-representation of the trustor (Luhmann, 1979: 39–40). The function of public relations is to mediate between organizations and their environment (Yang et al., 2016). In order to create transparency, organizations need public relations who mediate trustworthy cues in the form of concisely and understandable information about their open data applications. Public relations is therefore central to create transparency. As a result, public relations codes have the capacity to provide appropriate ethical guidelines that clarify how public relations professionals can achieve transparency regarding the use of open data. By applying existing public relations codes to the open data application process, we formulated 10 ethical guidelines on how organizations that control the collection and use of large amounts of open data can make their data use transparent. Using a fictive open-data-based smart city app, we then tested whether an organization that considers these guidelines and transparently provides information on its open data use is perceived as trustworthy. The results emphasize the importance of a transparent communication of open data applications and an ethical
Generating trust through information transparency to overcome privacy concerns

In online contexts, trust becomes vital when users perceive privacy risks when disclosing and sharing personal information (Chen et al., 2010; McKnight et al., 2011). Trust is a process based on the assessment of a trustee’s trustworthiness, upon which the trusting party decides whether they wish to be vulnerable to the actions of the trustee. Trustworthiness can be defined as the trusting party’s assessment of whether the trustee will perform a particular action important to them, regardless of their ability to monitor or control the trustee (Mayer et al., 1995; Söllner et al., 2012). It is a state, which does not automatically lead to an action as the behavioral manifestation of trust. Nevertheless, more trustworthiness increases the likelihood of action in which the trustor actually makes himself or herself vulnerable to the trustee (Wiencierz and Röttger, 2016). Whether or not trust is warranted only becomes clear in retrospect. In the research context, users as laypeople normally cannot assess whether the service provider uses open data in accordance with data protection laws and ethical standards. Users base their trust on a presumed compliance with such regulations. Thus, Luhmann (1979: 24) describes trust as a “risky investment.” Privacy concerns are therefore based on feelings of perceived vulnerability due to the collection and use of personal data, and the risk of potential and manifest information abuses (Dinev and Hart, 2004; Malhotra et al., 2004). This perceived vulnerability is where trust in organizations providing open data applications and services comes into play. Trust functions as the ability to tolerate these perceived risks (McKnight et al., 2011). Here, increased trust may compensate for perceptions of limited privacy; users are more willing to use service systems and are more likely to provide an organization with personal information when they trust it, despite potential privacy risks (Bol et al., 2018; Evjemo et al., 2019; Joinson et al., 2010; Martin and Murphy, 2017).

Studies show that many citizens in Western countries report privacy concerns when using online services (Eurobarometer, 2019; Pew Research Center, 2019). There is strong evidence that privacy concerns influence people’s willingness to disclose personal information and to use an online service (Cho et al., 2009; Joinson et al., 2010). The level of privacy required and the gravity of the concerns depend on the domain in which the data are generated (e.g. health care or e-commerce), individual differences (such as personality), and the type of personal information being disclosed (e.g. medical data or consumer behavior data). Non-individual differences also exert an influence, such as culture or the type of organization using the information (Bol et al., 2018; Cho et al., 2009; Dinev et al., 2013). An individual’s perception of the sensitivity of their information, the likelihood of its disclosure, and the severity of the resulting consequences all have a directly proportional relationship to the individual’s perception of the level of risk and privacy concerns involved (Dinev et al., 2013; Malhotra et al., 2004). Thus, whether privacy concerns exist when using online services and the level of these concerns is a subjective issue. At the same time, many people engage in extensive use of online services and share personal data, often ignoring privacy risks (Eurobarometer, 2019). Research on the
“privacy calculus” aims to explain the “privacy paradox,” suggesting that perceived monetary benefits and usefulness may outweigh privacy concerns (Barth and de Jong, 2017; Culnan and Armstrong, 1999). Thus, the use of online services also depends on the perceived advantages and benefits.

According to data protection regulations like General Data Protection Regulation (GDPR) in the European Union (EU) or statutory provisions of “Notice and Consent” in the United States, online service providers have to inform users about the generation and application of personal data (Solove and Schwartz, 2021). Furthermore, they can provide information about the usage of personal information that goes beyond the legally required transparency. Thus, by transparency, we understand the comprehensible provision of information about goals, ways and means of the generation, and use of open data. It does not refer to a hardly achievable all-encompassing transparency in the sense of publishing as well as explaining the source code of underlying software, algorithms, and all minute details of the data generation and processing. Organizations can provide such information in various ways in order to obtain users’ consent to use their data (Cate and Mayer-Schönberger, 2013; Liu, 2014). Research on whether enhanced transparency promotes users’ trust is divergent and controversial (Meijers et al., 2014; Susser, 2019). On one hand, there are indicators that information about the data collector’s intentions and cues like institutional privacy assurances may mitigate privacy concerns as they reduce the users’ risk perception (Oulasvirta et al., 2014; Xu et al., 2011). As Luhmann (1979: 39–40) emphasized, trust is influenced by the self-representation of the trustee. Transparent privacy policies about the types of information an organization collects and explanations as to how this information is used may be signals of trustworthiness, which affect trust formation positively (Chen et al., 2010; Martin and Murphy, 2017). On the other hand, transparency with regard to data privacy may evoke the perception of risks that the user was not previously aware of, and may lead to skepticism (Osterr et al., 2017). In particular, when organizations provide users with high levels of transparency about how they collect their data but low levels of control over said data, users perceive more privacy violation and have lower trust (Martin et al., 2017).

The research shows that the perception of privacy concerns as well as whether users deem the organization’s privacy policy to be sufficiently transparent differ between individuals. Information transparency evokes different levels of privacy concern in individuals, which, in turn, may lead to trust or skepticism. Compared to more traditional online services, open-data-based services may evoke the need for more transparency because freely accessible, sensitive user data are linked to various other data. The risk of privacy violation is higher because, primarily, there is the problem that even deleted personally identifiable information can potentially be restored in data records. This means that trust is more relevant in an open-data context. According to the divergent research, the question in the understudied context of open data is whether—and specifically what kind of—information transparency increases trust.

**Trustworthiness of open data-using organizations as a multifaceted construct**

Trust is based on the perceived trustworthiness of the trustee. Central antecedents to evaluate said trustworthiness are the trustee’s ability, integrity, and benevolence (Mayer
et al., 1995; Wiencierz and Röttger, 2016). However, “[H]uman-trust as traditionally conceptualized for dyadic relationships [...] cannot be easily applied because of imperfect knowledge and/or understanding of or familiarity with the service system, its actors and their agency” (Harwood and Garry, 2017: 445). In our research context, the antecedents of trustworthiness refer to the imperfect knowledge of the organization that uses open data. To analyze this imperfect knowledge, we have linked psychological findings surrounding the three antecedents with the findings of business information systems related to trust in IT artifacts.

Research in business information shows that the factor ability contains the organization’s perceived competence to program a functional, appealing app. This functionality refers to the user’s perception of whether the app has the functions or features needed to accomplish its task (Janson et al., 2013; Lankton et al., 2015). Competence in the area of data protection is also decisive for the research context (McKnight et al., 2011; Suh and Han, 2003). Ability therefore encompasses the user’s perception that the app provider, as the trustee, has the skills, competencies, and characteristics needed to have influence within the domain of data privacy.

In our research context, integrity reflects the trustor’s perception that the app provider adheres to a set of data privacy principles that are acceptable to the trustor (Lankton et al., 2015; Söllner et al., 2012). Whether users perceive the app provider as honest regarding its data application is crucial for the reflection of integrity (Harwood and Garry, 2017; Lankton et al., 2015). Furthermore, integrity refers to the app provider’s reliability, that is, the extent to which users believe that personal data are applied as indicated by the app provider (Söllner et al., 2012). Another related problem in this context is data security. Even if users believe that the app provider applies their data as indicated, vulnerability can be caused by a perceived lack of data protection measures (Harwood and Garry, 2017). Since our research project concerns strategic transparency regarding the use of data, the perceived quality of information, that is, the accuracy and completeness of the information about the use of data, is also important to the users’ perception of integrity (Janson et al., 2013; Kim et al., 2008).

Finally, benevolence is the trustor’s perception of whether the trustee wishes to do them good or is only driven by egocentric, profit-oriented goals (Harwood and Garry, 2017; Mayer et al., 1995). For example, if the app provider requests permission to use GPS data or to analyze text messages, benevolence refers to the users’ perception that the app provider will use these personal data in accordance with the users’ best interests.

**Guidelines for transparent communication for open data applications**

With public relations, organizations communicate strategically with their sociopolitical environment (political-administrative and sociocultural publics). Public relations brings the stakeholder perspective into the organization and also provides the organizational perspective to stakeholders. In the research context, the aim of public relations is to legitimize concrete open-data strategies and to ensure scope for action regarding the use of open data through social integration (Röttger et al., 2014). There is no organizational unit other than public relations that can mediate between the organization and its public,
and thus inform about the potentials and risks of open data through dialogue. Public relations creates public arenas in which every actor can contribute opinions, which in turn leads to a discourse. From the perspective of organizations as data collectors, their public relations professionals promote the acceptance of their open data applications through the strategic mediation of trustworthy cues in the sociopolitical environment. Accordingly, it is expedient to analyze this legitimacy work from a public relations perspective, including the codes of ethics of the profession. This article addresses the standards gap that exists with regard to how organizations should inform stakeholders in order to legitimize their use of open data, and describes 10 guidelines for transparent communication surrounding open data applications (see Figure 1; see also Wiencierz, 2018).

When using open data, organizations often link huge data assets with other data in real time. In the context of smart cities, for example, smart parking solutions are made possible by linking big data taken from sensors in parking spaces with user or vehicle geotracking data (Kitchin, 2014; Ojo et al., 2015). According to the understanding of open data presented here, these organizations make their real-time usage of open data transparent when they inform users about the typical steps of the big data application process: data generation, data processing, data analysis, and evaluation (Wiencierz and Röttger, 2019). Consequently, organizations should (1) reveal the purpose of their data usage. Regarding their data generation, they should (2) make the four big data characteristics transparent; they must inform users what data (variety) they collect in what volume and velocity and how reliable the generation is (veracity). In order for users to be able to assess the quality of the service, organizations should (3) provide information about the type of analysis they perform and (4) the reliability of the knowledge gained through their analyses (Wiencierz and Röttger, 2019). For example, a smart city app should provide information about whether open data are analyzed via deep learning techniques when making forecasts regarding traffic situations, and how reliable such forecasts are. Although data protection laws cover these four guidelines, users perceive the current transparency as insufficient, which fuels mistrust surrounding organizations’ data use (Eurobarometer, 2019).

The first four guidelines make transparent which data organizations generate and the way in which it is analyzed. The other six guidelines describe the ethical self-commitment necessary for data applications to communicate transparently, that is, ethical rules on how to inform users about the technical open data application process. They are based on public relations codes. These codes were developed to make public discourses transparent and comprehensible for everyone, meaning that they are also appropriate for describing ethical guidelines on how organizations should discuss their open data usage in order to create transparency. Codes of ethics in public relations, such as the *Code de Lisbonne* and *Code d’Athènes*, which are recognized by many public relations associations, summarize core values regarding ethical communication (Bowen, 2007; Public Relations Association of America, 2018; Röttger et al., 2014: 280). However, in the public relations profession, there are as yet no generally valid ethical guidelines on how to communicate in the context of big data or open data applications. By analyzing both aforementioned codes and the most important codes in Germany and the United States (the *German Communication Code* and the *Code of Ethics* from the Public Relations Society of America [PRSA], 2018, respectively), together with a study by Yang et al.
(2016) who compared the codes of ethics from 33 countries, we derived six additional guidelines on how to communicate in the context of open data. The supreme directive in all analyzed public relations codes is (5) strategic communication’s compliance with laws. In the context of open data, public relations professionals have to recognize data protection laws, for instance, when they notify users about which data they are generating. In addition, they have to show that their open data usage conforms with social norms (Richterich, 2018). In doing so, they obtain their license to operate, that is, the legitimation for their own business model (Martin and Murphy, 2017). The analyzed public relations codes emphasize openness, honesty, and truthfulness. Therefore, (6) organizations have to declare their open data applications as such and must willingly provide information about the collected (personal) information. The considered codes also emphasize that (7) public relations professionals should not deliberately mislead or confuse stakeholders by providing incomplete and distorted information. This means that they should not hide crucial information, such as uncertainties regarding the accuracy and reliability of the data or their analyses. The German Communication Code in particular emphasizes that (8) conscious discrimination against certain groups of people must be avoided. In doing so, organizations have to avoid depriving ethnic and religious groups of possible advantages when they inform users about the results of the open data analyses. Another shared value in all considered codes is expertise. This means that (9) public relations professionals have to demonstrate knowledge of open data tools and methods if they want to provide truthful information. Also vital in all analyzed codes is that (10) public relations professionals are always committed to the client and provide high-quality services to their client or employer. This guideline points out a putative contradiction: While transparency in open data applications must be created, trade and business secrets must be preserved to an appropriate degree. Organizations should allow as much transparency in breadth and depth as necessary to achieve legitimacy while ensuring that they survive competition and use their own strategic advantages.

Research question and hypothesis

In order to use open data productively despite the potential risks and vulnerability that this entails for citizens, law-abiding open-data organizations have to win trust by being transparent about which personal data are stored and how they are processed (Chen et al., 2010; Martin and Murphy, 2017). The trustee’s self-representation is central to building trust (Luhmann, 1979: 39–40). Thus, with the strategic communication of trustworthy cues about the use of open data, organizations may increase their perceived trustworthiness and encourage action from the trustor, for example, in the form of providing personal data or using the data-based services. This leads to our research question:

**Research Question:** How do differing degrees of transparency regarding the generation and application of open data influence users’ trust in the data-using organization?

In Europe, information about data generation and usage are required by law for any organization that may analyze user data. This information takes the form of privacy statements. The research shows that such information may lead to trust, but there are also
indicators that such information may evoke privacy fears. These results lead to two divergent hypotheses:

**Hypothesis 1a (H1a):** Information about the open data application process increases the perceived trustworthiness of organizations using open data.

**Hypothesis 1b (H1b):** Information about the open data application process decreases the perceived trustworthiness of organizations using open data.

We argue that the communication of ethical self-commitment to the transparent communication of data application forms trustworthy cues, as described by Luhmann (1979: 39–40).

**Hypothesis 2 (H2):** The communication of ethical self-commitment for the transparent communication of open data application promotes the perceived trustworthiness of the open data-using organization.

Of further importance is the analysis of the consequences that this perceived trustworthiness has on the user’s act of trust. Since our research focuses on an open-data-based app, we investigate the connection between the perceived trustworthiness of the app provider and the users’ intention to use this app:

**Hypothesis 3 (H3):** The more trustworthy users perceive the app provider to be, the more willing they are to use the app.

**Method**

**Study design**

The research question was addressed using an online survey experiment with a 2 (data application process: much vs little information) \( \times \) 3 (ethical self-commitment: much vs little vs no information) between-subject factorial design and a control group that had no information about the data application process and the ethical self-commitment of a fictive app named yourcity:app. This app promised to provide different services on the municipal level, such as intelligent traffic management, real-time parking and bus/train information, and weather forecasts. Such an app is representative of organizations within the smart city movement and provides a good example of the commercial and public use of open data, as the app serves all citizens, for example, by improving transit time and traffic flow (Ojo et al., 2015). At the same time, the usage of such sensitive data comes with potential risks to individual privacy (Green et al., 2017; Kitchin, 2014). The fictive app used in this study was based on the analysis of five actual apps from various German cities (e.g. Hamburg, Cologne) that help both inhabitants and visitors to navigate and use the cities’ facilities.

**Sample and procedure**

For sampling, we relied on the German Online Access Panel (OAP) of Respondi AG, an international provider of OAPs certified according to the ISO 26362 norm. Members of
The OAP were invited to participate in an online survey via email between 5 and 12 June 2018. They were offered a monetary incentive upon successful completion. After excluding participants who aborted the questionnaire and did not successfully pass the attention check, 783 respondents were distributed over seven conditions ranging in age from 17 to 81 years ($M = 47.73, SD = 14.53; 51.1\%$ female).

The survey began with sociodemographic questions (age, gender, and education) to randomly assign the participants to the experimental conditions, using interlocked quotas to allow for an equal gender distribution. The randomization was successful and identified no significant differences between the conditions concerning gender, $\chi^2(2, N=783) = 6.13, p = .409$, and age, $F(6, 776) = 0.48, p = .827$. This was followed by questions concerning the respondents’ consumption of media digitalization coverage and their individual risk disposition. Afterward, all respondents were shown the fictive landing page of yourcity:app along with information on the open-data-based app’s functionality, for example, the real-time mobility and news services. The stimulus came in the form of a second page from the same dynamic website, where the respondents were assigned to one of six experimental conditions and encountered the manipulation. The control group was not shown this second page but was instantly directed to the next questionnaire page, the manipulation check. Finally, all respondents answered questions on the perceived trustworthiness of the yourcity:app provider and their concrete intention to act, that is, their intention to use the app.

**Manipulation of independent variables**

Two experimental stimuli were presented in the survey: different amounts of information about (1) the app provider’s open data application process and (2) their ethical self-commitment to the transparent communication of data application. Based on the five actual apps that were analyzed, the condition with much information about data application addressed in detail which data the app provider collects while using the app, with what open data the provider combines these data, and how the provider protects its data in abidance with data protection laws. The condition with little information merely presented statements claiming that data protection is a matter of concern to the app provider and that the data applications conform to EU data protection regulations, with a link to the app’s general terms and conditions. We deliberately excluded the possibility of no information on the privacy policy because such statements are legally required in Europe for all organizations that collect and handle personal data (European Commission, 2019). In contrast, we allowed for a condition in which there was no information about ethical self-commitment at all, as such information is not legally required, and organizations present it at their discretion. The condition with much information about ethical self-commitment covered the six codes described in this article (see Figure 1) with detailed explanations of the respective codes. The condition with little information had a summary of the codes in the form of four bullet points, such as “No deception, misleading or discrimination of our users.”

**Assessment of dependent variables**

The dimensions of trustworthiness. To measure the perceived trustworthiness of the yourcity:app provider, we adapted trust scales regarding IT artifacts recently reported in
major journals, especially from business information systems to the open data context. To analyze the perceived ability of the app provider, we measured *competence in the area of data protection* (based on Lankton et al., 2015; \( \alpha = .97 \)) and *functionality* (based on Lankton et al., 2015; \( \alpha = .93 \)). To measure the perceived integrity of the provider, we analyzed the indicators *honesty* (based on Lankton et al., 2015; \( \alpha = .94 \)), *reliability* (based on Janson et al., 2013; McKnight et al., 2011; \( \alpha = .96 \)), *data security* (based on Janson et al., 2013; \( \alpha = .95 \)), and *quality of information* (based on Janson et al., 2013; Kim et al., 2008; \( \alpha = .96 \)). Finally, we measured the perceived *benevolence* (Janson et al., 2013; Lankton et al., 2015; \( \alpha = .94 \)). We geared the items toward a personal assessment of how the provider acts in relation to the problems associated with privacy risks and data security when using open data. We related the reported items directly to the provider of *yourcity:app*. For instance, to measure the app provider’s reliability, we changed the item “The app appears to be reliable” to “With regard to data protection, the provider of *yourcity:app* appears to be reliable.” All of the items were measured on a 7-point Likert-type scale (ranging from 1 = “do not agree at all” to 7 = “strongly agree”). To examine the seven hypothesized dimensions of trustworthiness, we calculated item intercorrelations, which ranged from \( r = .488 \) to \( r = .925 \).

To analyze the validity of the considered items regarding trustworthiness, we used three items (\( \alpha = .96 \)) based on Sun (2010), which universally address whether users would make themselves vulnerable to a trustee (e.g. “I would feel comfortable relying on the provider of *yourcity:app*”). We compared them with the aforementioned seven dimensions to measure the perceived trustworthiness of the *yourcity:app* provider. All dimensions correlate strongly with the universal evaluation of trustworthiness, ranging from Pearson’s \( r = .66 \) for the *functionality* dimension, to \( r = .86 \) for the *benevolence* dimension. When entered into a multiple linear regression, the seven trust dimensions explain 78.2% of the variance of trustworthiness, \( F(7, 775) = 401.62, p < .001 \). Even
though there is a certain level of multicollinearity, none of the variables used in the regression show a variance inflation factor (VIF) higher than a value of 10, which is the threshold suggested as worrisome by Myers (1990). Consequently, to account for the observed multicollinearity and to assess the extent to which the distinct trust dimensions are similarly affected, the multivariate analysis of variance (MANOVA) conducted hereafter is followed by a discriminant analysis.

Finally, we analyzed the perceived appeal and usefulness of yourcity:app with four self-formulated items (α = .96, for example, “I like yourcity:app”). Using a mean score index for what we assume to be the likability of the app, respondents in general appreciated the app (M = 4.94, SD = 1.39). It is due to this likability as well as the potential interest in and the attractiveness of the app that it becomes trust relevant.

**Intention to use yourcity:app.** Trust in the app provider includes users’ action, in which they make themselves vulnerable to the provider. As to whether or not respondents would actually make use of the app, four questions inquired about the intention to use yourcity:app (e.g. “I can envision using yourcity:app in everyday life”). All five items were measured on a 7-point Likert-type scale (ranging from 1 = “do not agree at all” to 7 = “strongly agree”). The items showed good internal consistency (α = .97, M = 4.63, SD = 1.64).

**Measurement of control variables**

**Risk disposition.** In the context of trust, the perceived risk and the individual risk disposition are of central importance as to whether users may use the app based on their previous evaluation of trustworthiness (Kim et al., 2008; Mayer et al., 1995). The risk disposition was measured using a single-item question (M = 3.80, SD = 1.44) that asked, “How do you see yourself—how willing are you in general to take risks?” and used a 7-point Likert-type scale, ranging from 1 = “not at all willing to take risks” to 7 = “very willing to take risks” (Beierlein et al., 2015).

**Consumption of media digitalization coverage.** Serving as a control for the respondents’ general interest and openness toward digital applications, respondents answered three questions concerning their consumption of media digitalization coverage: “How often do you follow news about digitalization (1) on television, (2) in newspapers and magazines, and (3) on the Internet?” Using a 5-point scale, respondents indicated their usage ranging from 1 = “never” to 5 = “very often.” The items showed acceptable internal consistency (α = .78, M = 2.88, SD = 0.84).

**Manipulation check**

For the manipulation check, respondents were asked how much information they received on the app’s website regarding the data application process and the app provider’s ethical self-commitment (1 = “no information,” 7 = “a lot of information”). The perceived amount of information on the data application process, $F(2, 780) = 83.04, p < .001$, and the provider’s perceived ethical self-commitment, $F(2, 780) = 95.65, p < .001$, differed
significantly between the conditions. Based on a Bonferroni post hoc test, the treatment groups with much information about the data application process ($M=5.26$, $SD=1.31$) and with little information ($M=4.85$, $SD=1.37$), and the control group ($M=3.24$, $SD=1.98$) differed significantly regarding their assessments of the amount of information perceived. The treatment groups with much information ($M=4.91$, $SD=1.29$) and with little information about the provider’s ethical self-commitment ($M=4.68$, $SD=1.36$) differed significantly from the group with no information and the control group ($M=3.31$, $SD=1.69$) in their assessments of the amount of information perceived. The manipulation can be evaluated as successful. There is no significant difference between the treatment groups with little and much information about ethical self-commitment.

**Findings**

The preliminary analysis shows high correlations between the items of all seven dimensions of perceived trustworthiness. Since the constructs were derived theoretically, we adhered to these constructs to investigate the effects of the manipulations on the app provider’s perceived trustworthiness. We conducted a two-way MANOVA using the varying degrees of information on the data application process and on the provider’s ethical self-commitment as the independent predictor variables, and the seven dimensions of perceived trustworthiness as dependent outcome variables. The analysis suggests that the variance–covariance matrices are not the same in all groups, as indicated by a significant Box’s test of the equality of the covariance matrices ($M=372.78$, $p<.001$). However, it has been suggested that this test can be disregarded when group sizes are equal (Field, 2009: 609). The results show that the amount of information on the data application process and on the provider’s ethical self-commitment affects all trustworthiness dimensions (see Tables 1 and 2). Using Pillai’s trace, the more information the respondents read about the data application process, $V=0.135$, partial $\eta^2=.068$, $F(14, 1542)=8.00$, $p<.001$, and ethical self-commitment, $V=0.04$, partial $\eta^2=.020$, $F(14, 1542)=2.42$, $p<.01$, the more trustworthy they perceived the yourcity:app provider to be in terms of the different trustworthiness dimensions. Following Cohen (1988), the trustworthiness dimensions are affected in a medium and small way by the amount of information on the data application process and the amount of information on the provider’s ethical self-commitment, respectively. However, using Pillai’s trace, there was no significant interaction effect between both independent variables on the trustworthiness dimensions, $V=0.020$, $F(14, 1542)=1.13$, $p=.322$.

To follow up on the MANOVA, we conducted a discriminant analysis and interpreted this as suggested by Field (2009: 615) to assess whether the dependent variables are affected similarly. The discriminant analysis revealed six discriminant functions, with the first one explaining 86.4% of the variance, canonical $R^2=.21$. The second function explained 6.8% of the variance, canonical $R^2=.02$. In combination, the discriminant functions significantly differentiated the treatment groups, $\Lambda=0.754$, $\chi^2(42)=219.18$, $p<.001$. Without the first function, results show that the five remaining functions did not significantly differentiate the treatment groups, $\Lambda=0.958$, $\chi^2(30)=32.90$, $p=.327$. Correlations between outcomes and the discriminant functions showed high to small loadings onto the first function (information quality, $r=.88$; reliability,
The discrimination plot suggests that the first function discriminated the six treatment groups from the no-treatment group. This result reflects the above findings from the MANOVA and confirms H1a, according to which information about the data application process increases the perceived trustworthiness of organizations that use open data. Consequently, H1b is disproved. The results also support H2, because the participants who read more information about the app provider’s ethical self-commitment perceived the organization as more trustworthy compared to those who read less or, in the case of the control group, received no information.

To analyze H3, that is, the influence of perceptions of trustworthiness on actual intentions to use yourcity:app, we conducted a multiple linear regression. The intention to use the app served as the dependent variable, while the composite trustworthiness score

### Table 1. Group differences of trust dimensions regarding information about the open data application process.

|                        | Control group (n=115) | Little information (n=331) | Much information (n=337) |
|------------------------|-----------------------|---------------------------|--------------------------|
|                        | M        | SD       | M        | SD       | M        | SD       |
| Competence in the area of data protection | 3.86<sup>a,b</sup> | 1.27 | 4.63<sup>a,c</sup> | 1.16 | 4.96<sup>b,c</sup> | 1.20 |
| Functionality          | 4.50<sup>b</sup> | 1.35 | 4.69<sup>c</sup> | 1.37 | 4.92<sup>b,c</sup> | 1.37 |
| Reliability            | 3.78<sup>a,b</sup> | 1.25 | 4.77<sup>a,c</sup> | 1.12 | 5.10<sup>b,c</sup> | 1.12 |
| Honesty                | 3.94<sup>a,b</sup> | 1.10 | 4.50<sup>a,c</sup> | 1.05 | 4.80<sup>b,c</sup> | 1.06 |
| Data security          | 3.78<sup>a,b</sup> | 1.20 | 4.44<sup>a,c</sup> | 1.12 | 4.73<sup>b,c</sup> | 1.18 |
| Information quality    | 3.64<sup>a,b</sup> | 1.30 | 4.72<sup>a,c</sup> | 1.20 | 5.16<sup>b,c</sup> | 1.11 |
| Benevolence            | 4.28<sup>b</sup> | 1.13 | 4.48<sup>c</sup> | 1.29 | 4.68<sup>b,c</sup> | 1.15 |

Mean values with identical letters differ significantly at <.05.

### Table 2. Group differences of trust dimensions regarding ethical self-commitment.

|                        | Control group and no information (n=331) | Little information (n=225) | Much information (n=227) |
|------------------------|------------------------------------------|---------------------------|--------------------------|
|                        | M        | SD       | M        | SD       | M        | SD       |
| Competence in the area of data protection | 4.36<sup>a,b</sup> | 1.26 | 4.80<sup>a</sup> | 1.20 | 4.97<sup>b</sup> | 1.16 |
| Functionality          | 4.68     | 1.37     | 4.79     | 1.43     | 4.86     | 1.32     |
| Reliability            | 4.40<sup>a,b</sup> | 1.28 | 4.95<sup>a</sup> | 1.13 | 5.13<sup>b</sup> | 1.07 |
| Honesty                | 4.28<sup>a,b</sup> | 1.08 | 4.69<sup>a</sup> | 1.06 | 4.78<sup>b</sup> | 1.09 |
| Data security          | 4.16<sup>a,b</sup> | 1.19 | 4.60<sup>a</sup> | 1.17 | 4.79<sup>b</sup> | 1.13 |
| Information quality    | 4.34<sup>a,b</sup> | 1.34 | 4.95<sup>a,c</sup> | 1.17 | 5.17<sup>b,c</sup> | 1.10 |
| Benevolence            | 4.42<sup>b</sup> | 1.10 | 4.60     | 1.15     | 4.64<sup>b</sup> | 1.20 |

Mean values with identical letters differ significantly at <.05.

$r = .79$; competency, $r = .63$; data security, $r = .59$; honesty, $r = .56$; functionality, $r = .20$; benevolence, $r = .24$). The discrimination plot suggests that the first function discriminated the six treatment groups from the no-treatment group. This result reflects the above findings from the MANOVA and confirms H1a, according to which information about the data application process increases the perceived trustworthiness of organizations that use open data. Consequently, H1b is disproved. The results also support H2, because the participants who read more information about the app provider’s ethical self-commitment perceived the organization as more trustworthy compared to those who read less or, in the case of the control group, received no information.
served as the independent variable. Controls used as independent variables in the regression analysis included gender, age, and education. In addition, we included the consumption of media digitalization coverage and the respondents’ general risk disposition.

The results support H3, according to which the app provider’s perceived trustworthiness is a strong predictor of the intention to use yourcity:app ($\beta = .61$). The more the respondents perceived the app provider as trustworthy, the more likely they were to use the app, even when controlled for gender ($\beta = .06$), general risk disposition ($\beta = .10$), and consumption of media digitalization coverage ($\beta = .12$). The regression model explains a large part of the variance with $R^2 = .43$ (Table 3).

**Table 3.** Multiple OLS regression models for the research question—dependent variable “intention to use yourcity:app.”

| Independent variable                        | $B$  | $SE(B)$ | $\beta$ | $t$  |
|--------------------------------------------|------|---------|---------|------|
| Age                                        | .00  | .00     | .01     | 0.42 |
| Gender                                     | .18  | .09     | .06     | 1.99*|
| Education                                  | .04  | .06     | .02     | 0.69 |
| Consumption of media digitalization coverage | .24  | .06     | .12     | 4.38***|
| Risk disposition                           | .11  | .03     | .10     | 3.50***|
| Perceived trustworthiness of the app provider | .92  | .04     | .61     | 21.74***|
| Constant                                   | -1.00| .32     | -3.14** |
| $N$                                        | 783  |         |         |      |
| $R^2$ adjusted                              | .43  |         |         |      |
| $F(6, 776) = 98.89$                        |      |         |         | ***  |

OLS: ordinary least squares.
Gender dummy-coded as 0 = “male” and 1 = “female.”

* $p < .05$; ** $p < .01$; *** $p < .001$.

Discussion

We have contributed to fulfilling the requirement for research into how organizations can convey transparency in the area of open data as well as offering an analysis of how users’ trust is influenced by transparency surrounding open data. A context- and situation-specific study is necessary in order to determine the effect of information transparency on trust in the data-sensitive open data context, as trust is subjective and situation-specific. The results suggest that in the context of an open-data-based app in the field of smart cities, information on the data application process as well as on ethical self-commitment to the transparent communication of data applications increases the app provider’s perceived trustworthiness. In turn, the more the respondents in this study perceived the app provider as trustworthy, the more inclined they were to use the app. The information provided on the data application process showed a stronger main effect on the trustworthiness dimensions than the information presented on the provider’s ethical self-commitment. One reason for this could be the greater familiarity with information on data applications in the form of privacy statements, which is regularly encountered when using online services. Encountering any references to the web service provider’s
law-abidance, regardless of how elaborately or briefly such information is conveyed, might suffice to evoke potential users’ trust. As an ethical self-commitment to the transparent communication of data applications is not legally binding, its perceived importance may appear to be less significant. It remains unclear whether the influence of such information is lower due to unfamiliarity or due to the perception of the app provider’s potentially lower commitment.

In the understanding of trust presented here, transparency is inherent to a certain extent in the antecedents of perceived trustworthiness, as integrity in particular concerns the perception of information on how the organization handles privacy. A certain degree of transparency is necessary for trust, otherwise users would not be able to assess trustworthiness. This does not mean that more transparency automatically increases perceived trustworthiness and leads to action, such as actually using open-data-based apps. The research shows that, first, there are different types of transparency and, second, that transparency is perceived differently from individual to individual. This means that the same information can be perceived and processed differently by different users, promoting both trust and skepticism. Our study shows that transparency about the use of open data is possible through the sober presentation of information on the technical data application process and on ethical self-commitment. These important, strategically communicated cues allow users to assess the organization’s trustworthiness. This insight is important for tackling the question of how to achieve legitimacy for the use of open data for the common good.

Implications

With our study, we have formulated guidelines on how service providers can create more transparency beyond that which is legally required in, for example, the EU GDPR regulations or the statutory provisions of “Notice and Consent.” We have shown that organizations can gain users’ trust via this extended transparency. In doing so, service providers that use open data can legitimate their open data usage and, finally, make public discourse about open data more transparent and comprehensible for everyone. With more trust via more transparency, service providers can ensure scope for their actions and legitimize their open data strategies through social integration.

Our considered antecedents of perceived trustworthiness clarify the trustworthiness cues for the use of open data that organizations should emphasize in their strategic communication in order to gain trust. By using items from business information systems and psychology and transferring them to the communication science research context, we took an interdisciplinary approach to trust. The analysis of our approach shows that open-data organizations should highlight their benevolence and their ability, such as the functionality of their open-data services. They appear to have integrity when they provide trustworthy, honest cues that assure users that their data are used as indicated and are stored securely. At the same time, there is the limitation that these factors have not proven to be selective, as the high intercorrelations show. Further studies should research whether users really perceive different dimensions of trustworthiness—also in contexts beyond a specific smart city app.
In its function as a mediator, public relations acts as a bridge that crosses boundaries by facilitating a societal discussion between the various actors involved in open data, such as politicians, company representatives, or data privacy activists. By monitoring the expressed expectations regarding open data, these actors can use their public relations to influence the discussion surrounding values and standards and articulate their own interests. Thus, public relations is important for the exchange of expectations about open data between the respective actors and stakeholders, as well as for the social learning process about the provision and application of open data. From our point of view, generally valid ethical guidelines on how to make the application of open data transparent are indispensable for a data society, since large amounts of data also entail a great deal of responsibility. Because of its own perception as a mediator between individuals, groups, and organizations and society (Yang et al., 2016), public relations should formulate guidelines on how organizations should inform their stakeholders about the application of open data. Furthermore, as our results suggest, the profession should communicate them openly and proactively to all concerned, as such transparency helps to build trust in this context and may ultimately increase the legitimacy of open data. With our theoretically derived ethical guidelines, we have made an important initial step in the discussion about which guidelines public relations should formulate in the context of open data. However, our proposals need to be presented to practitioners in order to examine the extent to which they are practicable and implementable in cases of ethical problems or doubt when using open data.

The obvious privacy risks that will always accompany open data are not to be neglected. Organizations also have a duty to inform users of such risks. Thus, if the benefits of open data for the public are to be utilized—for instance, in building smart cities—stakeholders are automatically exposed to potential risks concerning individual privacy. It remains to be discussed what risks or degree of risk should be taken in order to exploit open data’s enormous potential. Therefore, the discussion should not aim for blind trust, but trust with healthy skepticism. Users as laypeople are dependent on the information that organizations provide about their use of open data. When organizations communicate according to our derived guidelines, it will become easier for users to assess whether the use of open data complies with the relevant laws and values. Ultimately, as laypeople they can never be absolutely sure whether service providers are taking advantage of them. Only legal and ethics experts can evaluate this. For this assessment, experts also need information from the organizations that use open data. With our ethical guidelines, we have made a proposal on how to make the use of open data more transparent.

Acknowledgements

Christian Wiencierz would like to thank the State of North Rhine-Westphalia’s Ministry of Economic Affairs, Innovation, Digitalization, and Energy as well as the Exzellenz Start-up Center. NRW program at the REACH—EUREGIO Start-Up Center for their kind support of his work.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research is funded by the German Society for Online Research.
ORCID iD

Christian Wiencierz iD https://orcid.org/0000-0001-9231-2404

References

Ada Lovelace Institute (2020) No green lights, no red lines: public perspectives on COVID-19 technologies. London. Available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2020/07/No-green-lights-no-red-lines-final.pdf

Barth S and de Jong MDT (2017) The privacy paradox—investigating discrepancies between expressed privacy concerns and actual online behavior—a systematic literature review. Telematics and Informatics 34(7): 1038–1058.

Beierlein C, Kovaleva A, Kemper CJ, et al. (2015) Kurzskala zur Erfassung der Risikobereitschaft (R-1) [Short scale to measure the willingness to take risks]. GESIS Working Papers 2014|34. Cologne: GESIS. Available at: https://search.gesis.org/instruments_tools/zis236

Bol N, Dienlin T, Kruikemeier S, et al. (2018) Understanding the effects of personalization as a privacy calculus: analyzing self-disclosure across health, news, and commerce contexts. Journal of Computer-Mediated Communication 23(6): 370–388.

Bowen S (2007) Ethics and Public Relations. Institute for Public Relations. Available at: https://instituteforpr.org/ethics-and-public-relations/ (accessed 12 January 2018).

Cate FH and Mayer-Schönberger V (2013) Notice and consent in a world of big data. International Data Privacy Law 3(2): 67–73.

Chen YH, Chien SH, Wu JJ, et al. (2010) Impact of signals and experience on trust and trusting behavior. Cyberpsychology, Behavior, and Social Networking 13(5): 539–546.

Cho H, Rivera-Sánchez M and Lim SS (2009) A multinational study on online privacy: global concerns and local responses. New Media and Society 11(3): 395–416.

Cohen J (1988) Statistical Power Analysis for the Behavioral Sciences. 2nd ed. Hillsdale, NJ: Lawrence Erlbaum.

Culnan MJ and Armstrong PK (1999) Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organization Science 10(1): 104–115.

De Montjoye YA, Radaelli L, Singh VK, et al. (2015) Unique in the shopping mall: on the reidentifiability of credit card metadata. Science 347(6221): 536–539.

Dinev T and Hart P (2004) Internet privacy concerns and their antecedents—measurement validity and a regression model. Behaviour and Information Technology 23(6): 413–422.

Dinev T, Xu H, Smith HJ, et al. (2013) Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems 22: 295–316.

European Commission (2019) Regulation (EU) 2016/679. General Data Protection Regulation. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN

Eurobarometer (2019) The General Data Protection Regulation. Special Eurobarometer 487a. Available at: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/86886

European Commission (2019) Regulation (EU) 2016/679. General Data Protection Regulation. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN

Evjemo B, Castejón-Martínez H and Akselsen S (2019) Trust trumps concern: findings from a seven-country study on consumer consent to “digital native” vs. “digital immigrant” service providers. Behaviour & Information Technology 38(5): 503–518.

Field A (2009) Discovering Statistics Using IBM SPSS Statistics. Los Angeles, CA: SAGE.
Green B, Cunningham G, Ekblaw A, et al. (2017) *Open Data Privacy*. Berkman Klein Center for Internet and Society Research Publication. Available at: http://nrs.harvard.edu/urn-3:HUL.InstRepos:30340010

Harwood T and Garry T (2017) Internet of things: understanding trust in techno-service systems. *Journal of Service Management* 28(3): 442–475.

Janson A, Hoffman A, Hoffmann H, et al. (2013) *How Customer Trust Mobile Marketing Applications*. In: 34th international conference on information systems, Milan, Italy. Available at: https://pdfs.semanticscholar.org/be39/cea8259e7d109652ed2311e99b3af4898f11.pdf

Joinson AN, Reips UD, Buchanan T, et al. (2010) Privacy, trust, and self-disclosure online. *Human-Computer Interaction* 25(1): 1–24.

Kim DJ, Ferrin DL and Rao HR (2008) A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. *Decision Support System* 44(2): 544–564.

Kitchin R (2014) The real-time city? Big data and smart urbanism. *GeoJournal* 79(1): 1–14.

Lankton NK, McKnight DH and Tripp J (2015) Technology, humanness, and trust: rethinking trust in technology. *Journal of the Association for Information Systems* 16(10): 880–918.

Leins K, Culnane C and Rubinstein BI (2020) Tracking, tracing, trust: contemplating mitigating the impact of COVID-19 with technological interventions. *The Medical Journal of Australia* 213(1): 6–8.e1.

Liu Y (2014) User control of personal information concerning mobile-app: notice and consent? *Computer Law & Security Review* 30(5): 521–529.

Luhmann N (1979) *Trust and Power: Two Works by Niklas Luhmann*. Chichester: Wiley.

McKnight DH, Carter M, Thatcher JB, et al. (2011) Trust in a specific technology: an investigation of its components and measures. *ACM Transactions on Management Information Systems* 2(2): 12.

Malhotra NK, Kim SS and Agarwal J (2004) Internet Users’ Information Privacy Concerns (IUIPC): the construct, the scale, and a causal model. *Information Systems Research* 15(4): 336–355.

Martin KD, Borah A and Palmatier RW (2017) Data privacy: effects on customer and firm performance. *Journal of Marketing* 81(1): 36–58.

Martin KD and Murphy PE (2017) The role of data privacy in marketing. *Journal of the Academy of Marketing Science* 45(2): 135–155.

Mayer RC, Davis JH and Schoorman FD (1995) An integrative model of organizational trust. *Academy of Management Review* 20(3): 709–734.

Meijers R, Conradie C and Choenni S (2014) Reconciling contradictions of open data regarding privacy, transparency, security and trust. *Journal of Theoretical and Applied Electronic Commerce Research* 9(3): 32–44.

Myers RH (1990) *Classical and Modern Regression with Applications*. 2nd ed. The Duxbury Advanced Series in Statistics and Decision Sciences. Belmont, CA: Duxbury Press.

Ojo A, Curry E and Zeleti FA (2015) A tale of open data innovations in five smart cities. In: 48th Hawaii international conference on system sciences, Kauai, HI, 5–8 January. IEEE. Available at: https://ieeexplore.ieee.org/document/7070094

Open Knowledge International (2018a) Open definition 2.1. Available at: http://opendefinition.org/od/2.1/en/ (accessed 25 January 2018).

Open Knowledge International (2018b) About. Available at: https://okfn.org/about/ (accessed 25 January 2018).

Ostherr K, Borodina S, Bracken RC, et al. (2017) Trust and privacy in the context of user-generated health data. *Big Data and Society*. Epub ahead of print 17 April. DOI: 2053951717704673.
Oulasvirta A, Suomalainen T, Hamari J, et al. (2014) Transparency of intentions decreases privacy concerns in ubiquitous surveillance. Cyberpsychology, Behavior, and Social Networking 17(10): 633–638.

Pew Research Center (2019) Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Available at: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Public Relations Society of America (PRSA) (2018) Code of ethics. Available at: https://www.prsa.org/ethics/code-of-ethics/ (accessed 12 January 2018).

Richterich A (2018) The Big Data Agenda: Data Ethics and Critical Data Studies. CDSMS, Critical Digital and Social Media Studies. London: University of Westminster Press.

Röttger U, Preusse J and Schmitt J (2014) Grundlagen der Public Relations. 2. Auflage [Basics of Public Relations]. Wiesbaden: VS Verlag für Sozialwissenschaften.

Scholz TM (2017) Big Data in Organizations and the Role of Human Resource Management. A Complex Systems Theory-Based Conceptualization. Frankfurt: Peter Lang GmbH.

Söllner M, Hoffmann A, Hoffmann H, et al. (2012) Understanding the formation of trust in IT artifacts. In: 33rd international conference on information systems (ICIS), Orlando, USA. Available at: https://www.alexandria.unisg.ch/219845/

Solove DJ and Schwartz PM (2021) Information Privacy Law. 7th ed. Aspen casebook series. New York: Wolters Kluwer.

Suh B and Han I (2003) The impact of customer trust and perception of security control on the acceptance of electronic commerce. International Journal of Electronic Commerce 7(3): 135–161.

Sun H (2010) Sellers’ trust and continued use of online marketplaces. Journal of the Association for Information Systems 11(4): 182–211.

Susser D (2019) Notice after notice-and-consent: why privacy disclosures are valuable even if consent frameworks aren’t. Journal of Information Policy 9: 37–62.

Wiencierz C (2018) Vertrauen in gemeinwohlorientierte Big-Data-Anwendungen. Ethische Leitlinien für eine datenbasierte Organisationskommunikation [Trust in big data applications for the common good. Ethical guidelines for a data-based organizational communication]. In: Liesem K and Rademacher L (eds) Die Macht der Strategischen Kommunikation. Mediennetische Perspektiven der Digitalisierung [The power of strategic communication. Media Ethical Perspectives of Digitalization]. Baden-Baden: Nomos, pp. 109–126.

Wiencierz C and Röttger U (2016) Trust in organizations—the significance and measurement of trust in corporate actors. In: Blöbaum B (ed.) Trust and Communication in a Digitized World. Models and Concepts of Trust Research. Berlin: Springer, pp. 91–111.

Wiencierz C and Röttger U (2019) Big data in public relations: a conceptual framework. Public Relations Journal 12(3): 1–15.

World Economic Forum (2012) Big Data, Big Impact: New Possibilities for International Development. Cologne and Geneva. Available at: http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf

Xu H, Dinev T, Smith J, et al. (2011) Information privacy concerns: linking individual perceptions with institutional privacy assurances. Journal of the Association for Information Systems 12(12): 798–824.

Yang A, Taylor M and Saffir AJ (2016) Ethical convergence, divergence or communitas? An examination of public relations and journalism codes of ethics. Public Relations Review 42(1): 146–160.

Zuboff S (2019) The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power. London: Profile Books.
Author biographies

Christian Wiencierz is the executive assistant in the start-up center REACH at the University of Münster. His research focuses on strategic communication, Big Data, agile development, and trust.

Marco Lünich is a postdoctoral researcher at the University of Düsseldorf, Germany. His research focuses on public perceptions and social consequences of digital media, Big Data, and Artificial Intelligence.