Computers in Human Behavior 122 (2021) 106830

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: http://www.elsevier.com/locate/comphumbeh

Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security

Lyn E. Pleger [*], Katharina Guirguis, Alexander Mertes

Institute of Public Management, Zurich University of Applied Sciences, Bahnhofplatz 12, 8401, Winterthur, Switzerland

ARTICLE INFO

Keywords:
Data security
Data protection
Information privacy
User perspective
Comparison
UK
Germany
E-government

ABSTRACT

Digitisation processes in the public sector have led to an increase in innovative approaches for better service delivery using information and communication technology. Citizens, however, often have reservations towards e-government efforts due to concerns regarding data protection (DP) and data security (DS). This article is based on a mixed-methods design consisting of a media analysis and an online survey of 1000 respondents from the UK and Germany, which investigates the conception of DP and DS from the citizens' point of view. Results demonstrate that citizens do not fully understand the terminology used in newspaper articles concerning DP and DS. Moreover, findings show that DP and DS are of great importance to citizens. However, the perceived relevance of DP and DS varies between services, being strongest for online banking. Compared to the German citizens surveyed, the UK citizens displayed greater concerns about disclosing personal data online. Despite some differences, however, findings across both samples indicate a common lack of understanding of the two concepts DP and DS. The resulting citizen concept of DP and DS can help to mediate between politics, technology and the public in the discourse of e-government initiatives and the requirements for DP and DS. We argue that citizens' understanding of DP and DS is a prerequisite for governments to adequately address citizens' concerns regarding e-government initiatives.

1. Introduction

Digitisation processes in the public sector have led to an increase in innovative approaches for better service delivery (see e.g., Wilkowska & Ziefle, 2012). The umbrella term describing the promotion of better public service delivery by means of information and communication technology (ICT) is *e-government*. When delivering a public service, citizens and their requirements as stakeholders are of particular focus. Of especially high importance are data protection (DP) and data security (DS) as the state has a special obligation to secure and protect the data of citizens. The state creates the context and implements the legal provisions for companies to protect users' data. In this sense, Combe (2009, p. 395) argues that "[in] a civil society, privacy safeguards are a cornerstone of basic human rights and are enshrined in a series of legislative measures to ensure standards are adhered to by recipients of personal information, be they public or private organisations, or individuals." A state, therefore, creates the context and implements the legal provisions for companies to protect their customer data. Governments aiming at an "information society" need to not only treat concerns of their citizens seriously but should also address them proactively and continuously (Lips et al., 2005, p. 1).

Considering that citizens produce data continuously and that they are usually unable to opt out of having their data collected, the state's role in safeguarding DP and DS becomes even more significant. Citizens are often not free to decide whether they want to produce data or not – an issue which is also closely linked to internet users' trade-offs "regarding online data collection and privacy" (Aïmeuret al., 2013, p. 237).

Against this background, it is not surprising that online privacy has become an increasingly important issue for citizens (Aïmeuret al., 2013; Wolters, 2019). Research shows that citizens are often positive about e-government efforts (United Nations, 2018; Ma & Zheng, 2017). What is striking, however, is the consensus on citizens' concerns about e-government-related initiatives. Study results reveal that reservations concerning e-services or e-government in general are often based on concerns related to DP and DS (Romanou, 2018; Spiekermann et al., 2015; Tsavli et al., 2015). For instance, studies have repeatedly shown that DP and DS are of great importance for citizens in the context of ICT

[*] Corresponding author.
E-mail address: lyn.pleger@zhaw.ch (L.E. Pleger).

https://doi.org/10.1016/j.chb.2021.106830
Received 14 February 2020; Received in revised form 31 March 2021; Accepted 14 April 2021
Available online 17 April 2021

implementation (Brodie et al., 2005, pp. 35–43; Combe, 2009; Hallinan et al., 2012; Joinson et al., 2006; Malhotra et al., 2004; Palen & Dourish, 2003; Pleger et al., 2020; Yun et al., 2019).

Despite the perceived relevance of DP and DS, it is surprising that there is no common understanding, neither among researchers nor among practitioners, as to what exactly is meant by the terms (Hallinan et al., 2012; Tamò-Larrieux, 2019). One reason for the lack of consensus arguably stems from the fact that DP and DS are elusive concepts that can be approached from different perspectives. Users, regulators and policy makers each have different views on the different perspectives of DP and DS, making a clear distinction even more challenging (Ortlieb & Garner, 2016).

There are fundamental differences between DP and DS. A distinction between the two concepts is important for several reasons that concern both the state as a service provider and the citizens as end-users: First, in order to have a discourse that reaches the population it is essential to investigate the level of information of the population regarding DP and DS in order to shape the public discourse on the important issue of information privacy in such a way that the majority of end-users can follow the discourse. It is, therefore, not primarily a question of citizens being able to formally name the (academic) differences between DP and DS. Rather, knowledge of the differences serves as an indicator of citizens' knowledge of the topic as a whole. The conceptual mixing of DP and DS is a symptom of a much deeper problem, containing a normative and a practical component: In a broader democratic-theoretical sense, the knowledgeability of citizens contains a normative component in that a democracy requires the participation of citizens. Participation, in turn, requires being informed. In the narrower practical sense, citizens cannot fulfil their responsibility of taking sufficient precautions when using the internet if they are not well-informed. Only if citizens are able to follow and understand the public discourse are they able to form a well-founded opinion. For these reasons, the knowledge of citizens about the formal distinction between DP and DS is important. While studies exist that examine the end-user perspective towards the perceived security and privacy concerns when using the internet (see e.g., Distler et al., 2020; Rainie & Duggan, 2015), far less research has focussed on a clear distinction between DP and DS. More precisely, there is a lack of empirical studies on the state of information of the population regarding the concepts of DP and DS and their distinctive factors.

This article therefore aims to help conceptualise DP and DS from the population point of view by means of an empirical study which addresses the following research questions: What do citizens mean by the terms DP and DS? How familiar are citizens with the terminology used in the media in the context of DP and DS? To what extent does citizen understanding (i.e., the subjective perspective) coincide with the technical and legal perspectives of the terms? The main contribution of this study is to provide a basis for policymakers to better tailor initiatives to the needs of citizens by better understanding their perspective on DP and DS.

The study is based on a mixed-methods design to address the research objectives in two consecutive steps. In a first step, a media analysis is used to investigate whether a distinction is made between DP and DS in public discourse and which technical terms are related to DP and DS. Based on the results of the media analysis as well as theoretical derivations, in a second step, a survey was conducted to investigate whether citizens are aware of the differences between DP and DS and to what extent they are generally familiar with the topic and related concepts. The survey's respondents consist of 1,000 citizens from the UK and Germany. Collecting responses from two different countries also allows to assess differences and similarities among the perceptions of citizens within different political and legal environments.

The article is structured as follows: First, an overview of the three perspectives of DP and DS and the state of research is given, before turning to the research design of this article. After presenting the methodology of the media analysis, the survey design is described and findings are presented. The results are interpreted in the discussion and embedded within the larger theoretical and practical context. The conclusion sums up the results and emphasises the potential for further research.

2. Data protection and data security

DP and DS are complex concepts and research lacks a uniform definition of these terms (Hallinan et al., 2012). In theory and practice a clear distinction is often not made between the two terms DP and DS, although they have different meanings. The complexity of the topic and the interchangeable use of different terms might lead to an understanding of the concepts of DP and DS among citizens which varies from the legal and technical perspectives. The potential existence of different perspectives emphasises the importance of including public understanding in the discourse. Citizens' concerns can only be taken seriously and represented in political measures if they are identified and addressed adequately. An underlying assumption of this article is that citizens' understanding (i.e., the subjective perspective) is influenced by the technical and the legal perspectives, and citizens thus do not distinguish between the two concepts DP and DS. The subjective perspective plays an important role for a holistic perspective on the concepts of DP and DS. Scholars agree that DP and DS are of great importance to individuals (Hallinan et al., 2012; Joinson et al., 2006; Lynskey, 2014). While there is research that aims to understand the mental model of users in the context of DP and DS (Bergström, 2015; Lin et al., 2012), little is known about citizens' literal understanding of the concepts of DP and DS, which we argue is an aspect that needs to be taken into consideration to understand the diffuse concepts of DP and DS from a subjective point of view. A careful conceptualisation is further of great importance, particularly for research purposes, as constructs such as DP and DS represent abstract phenomena that first need to be conceptualised to be investigated (MacKenzie et al., 2011).

MacKenzie et al. (2011, p. 299) suggest four factors that need to be considered in construct conceptualisation: 1) assessment of how the construct has been used in previous research, 2) specification of the nature of the construct's conceptual domain, 3) specification of the construct's theme, and 4) unambiguous definition of the construct. Following these suggestions, based on previous research, we specify the nature and theme of the conceptual domain to provide a definition of the concepts DP and DS.

Previous research states that *data protection* focuses on personal data in the sense of informational self-determination and therefore relates to legal regulations (Lynskey, 2014). *Data security,* on the other hand, emphasises the technical components of data management (DiMase et al., 2015). DP and DS thus address two different perspectives of how public or private organisations handle the personal data of citizens or customers. The nature of the construct's domain is defined by the "property the construct represents, and the entity to which it applies" (MacKenzie et al., 2011, p. 299). The *property* thereby is "the phenomena to which the construct refers" and the *entity* is "the object to which the property applies" (MacKenzie et al., 2011, p. 298). In the case of DP and DS, the nature of the constructs' domains can be described as follows: While both concepts deal with 'data' as their entity, they refer to different properties as DP covers data protection from a legal point of view, whereas DS is concerned with its technical security. The theme of a construct is characterised by the description of attributes it can be described with (MacKenzie et al., 2011). In the case of DP, this is mainly the legislation it manifests itself in and in the case of DS, these are technical measures to prevent data misuse.

This article proposes a conceptual framework for DP and DS that distinguishes between the concepts on the basis of different perspectives. Firstly, there is a *legal perspective* (see, e.g., John, 2018) relating to DP that is primarily explored by administrations and politicians, mainly in the context of legislation. Secondly, a *technical perspective* (Fischer & Hofer, 2011; Pfleeger et al., 2015), which refers to DS, is primarily held by technicians dealing with technical aspects, such as cyber security.

The third perspective is the *subjective perspective*, which is the subject of this study, and comprises the integral conceptualisation of DP and DS by the citizens. The latter is often much less concrete than the other perspectives and is based on intuition rather than facts. Insight into citizen understanding of DP and DS helps to mediate between politics, technology, and the public in the discourse of e-government initiatives and the requirements for DP and DS. In the following subchapters, a definition of all three perspectives is provided, completing MacKenzie et al.'s (2011) recommended factors for construct conceptualisation.[1].

2.1. The legal perspective

The legal perspective represents data protection from a legal point of view and refers to the legal framework (e.g., laws, acts and regulations) dealing with the protection of data. Examples for such legal frameworks include the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016), the Data Protection Act (DPA) in the UK, or the Bundesdatenschutzgesetz (BDSG) in Germany.

The terms *data protection* and *privacy* are often intertwined or used synonymously (Bennett, 1992; Hallinan et al., 2012; Hoepman, 2014). However, Lynskey (2014) emphasises that it is important to distinguish between the two terms since data protection goes further and provides the individual with more control than privacy. Data protection "promotes the right to personality of individuals through informational self-determination and […] reduces the information and power asymmetries which can have a negative impact on individual autonomy" (Lynskey, 2014, p. 597). Privacy deals with the right to private life whereas data protection addresses the rights of the individual and, as such, more aspects are covered by the latter (Kokott & Sobotta, 2013). The EU initiated harmonisation efforts regarding data protection among its member states resulting in the introduction of the General Data Protection Regulation (GDPR) on May 25, 2018 (Wolters, 2019). The GDPR implementation aimed at enhancing the protection of personal data and at strengthening "consumers' rights to data privacy" (Presthus & Sørum, 2019, p. 19; see also; Wolters, 2018). Goddard (2017, p. 703) emphasise the impact of this enhancement by stating that "based on the concept of privacy as a fundamental human right (as enshrined in the Charter of EU Rights), the Regulation will have wide global impact." In the UK, GDPR is incorporated in the Data Protection Act (Data Protection Act, 2018). In Germany, the Bundesdatenschutzgesetz applies the GDPR to national law (Bundesdatenschutzgesetz 2017, 2018, p. 2018).

2.2. The technical perspective

While the legal perspective focuses on data protection legislation, the technical perspective refers to aspects of data security. Historically, the term *data security* was introduced in the 1980s by technical and legal experts and later came into common parlance (Bennett, 1992). The differentiation between DP and DS emerged due to the advances in technology (Bennett, 1992).

In contrast to data protection, which deals with the legal assessment of data processing, data security is concerned with technology being designed to allow automated data processing to be automatically compliant with law (Roβnagel, 2007). Both concepts, however, manifest themselves in legislation. For example, in Article 32 of the GDPR it is stated that data controllers and processors are obliged to undertake "technical and organisational measures to guarantee the safeguard of personal data" (Voigt & von dem Bussche, 2017, p. 38). Data security covers the organisational, constructional and/or technical measures in place to protect stored or transmitted data from unwanted human, natural or technical interference (DiMase et al., 2015; Fischer & Hofer, 2011). Security has to be guaranteed and protected from both accidental or intentional unauthorised access (DiMase et al., 2015). Data security is also referred to as "technical data protection" (Richter, 2012). Examples of data security measures are privacy enhancing technologies, such as cookie management software or encryption technologies (Phillips, 2004). With regard to data shared with the state – for example through the use of e-government services – data security is of particular importance as, in case of breaches, very sensitive data could be affected (Wu, 2014).

2.3. The subjective perspective

The subjective perspective covers aspects of DP and DS from an individual's or end-user's perspective. In contrast to the legal and the technical perspective where the "entity to which [the] construct applies" is *data*, the entity concerned in the subjective perspective is the *individual* (see MacKenzie et al., 2011, p. 298). When trying to capture the subjective perspective, it becomes evident that the academic debate on DP and DS does often not explicitly include the users' perspectives (Friedewald et al., 2017; Hallinan et al., 2012). The literature that does exist shows that the public (literal) understanding of the issues of DP and DS is rather limited but that awareness is increasing due to greater sensitivity towards data breaches and unethical data handling (Rempel et al., 2019). Several aspects of data security have proven to be relevant for data subjects, such as security (e.g. Distler et al., 2019; Spiekermann, 2012), privacy (e.g. Brodie et al., 2005, pp. 35–43; Brough & Martin, 2019; Distler et al., 2020), perceived control over personal data (e.g., Dogruel & Joeckel, 2019; van Ooijen & Vrabec, 2019), trust and risk perception (e.g., Landwher, 2019) and cultural backgrounds (e.g., Krasnova, Veltri, & Günther, 2012). To provide a better understanding of the subjective perspective, these aspects are described in more detail in the following.

Security concerns

When addressing the subjective perspective, citizens' perceived security as a substantial human need is of particular importance (Sheldon et al., 2001). In the early 1990s, system end-users did not seem particularly concerned about their security (Goodhue & Straub, 1991). Today, even though their knowledge of security is often limited, users are generally aware of the security risks that accompany new technologies (Distler et al., 2019, p. 11). Security concerns can be defined as concerns attributed to the "protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of information system resources" (Zafar, 2013, p. 106).

Privacy concerns

While security is often quite specific, privacy is a "fuzzy concept" (Spiekermann, 2012, p. 39) that has generated more awareness with the introduction of new technologies (Palen and Dourish, 2003). "Privacy is about the scarcity of personal data creation and the maximization of individuals' control over their personal data" (Spiekermann, 2012, p. 40). Accordingly, privacy concerns describe "individuals' motivation to protect personal information from unauthorized access" (Brough and Martin, 2019, p. 1). They seem to be a major issue for web users (Malhotra et al., 2004; Preibusch, 2013), and the concept of privacy and corresponding concerns have resulted in research from different disciplines (see e.g., Brough & Martin, 2019; Chang et al., 2018; Jozani et al., 2020; Margulis, 2003; Preibusch, 2013; Tavani, 2007; Wagner & Eckhoff, 2018). The nature of privacy concerns can be summarised as a "worry about the consequences of the different usages of their personal data and the use of erroneous or incomplete data" (see also Dogruel & Joeckel, 2019; Rohunen & Markkula, 2019, p. 487). In the context of online-based data, the term "information privacy" arose to describe privacy issues when using the internet (Malhotra et al., 2004, p. 337; Preibusch, 2013, p. 1134). Yun et al. (2019p. 572) emphasise that

[1] For the subjective perspective no unambiguous definition can be provided as this perspective is much less concrete than the other ones. One aim of this article is to reduce this ambiguity by investigating the phenomenon of the subjective perspective.

privacy concern is not a new phenomenon but that concerns about personal information privacy "have evolved significantly with time in part due to the emergence of disruptive technologies".

Perceived control over personal data

As individual control can be seen as a "reflection of fundamental values such as autonomy, privacy and human dignity" (van Ooijen & Vrabec, 2019, p. 92), research and practice agree that subjects should have some control over the use of their personal data. Custers et al. (2018, p. 238) found that only 15% of EU citizens feel in full control of their personal data. In their international comparison of different countries, they found that while German citizens were below this average, UK citizens were above average and thus perceived to be more in control of their data. Perceived control over one's own data is closely linked to data privacy concerns (Yun et al., 2019).

Trust and risk perception

The increasing importance of trust and risk beliefs for users, along with an increasing use of ICT, is undisputed in research (e.g., Malhotra et al., 2004). These concepts of trust and risk beliefs are of particular importance in the context of public administration and government. More than a decade ago, Lips et al. (2005, p. 1) posited that "[r]isk and trust must be acknowledged as central concepts in governments' ambitions to address the information society." Since then, determinants of citizens' privacy concerns, such as trust and risk, have received considerable attention and been the subject of several empirical studies. Overall, "privacy behavior" of individuals is understood to be a consequence of individuals' privacy risk perceptions (Dogruel& Joeckel, 2019, p. 1768). For users to be willing to provide personal information online, they must have confidence that their data will not be misused (Landwher, 2018).

Cultural background

Culture plays a crucial role in an individual's behaviour when using the internet as well as regarding their privacy concerns (Krasnovaet al., 2012; Widjaja et al., 2019). [Cultural] values can be understood as "underlying mechanisms" impacting citizens' judgments of what is of personal importance and ultimately their social behaviour (Hoffman & Slater, 2007, p. 59; see also Hofstede, 2001) and thus how citizens deal with privacy (Dogruel& Joeckel, 2019). Empirical findings regarding the influence of culture on privacy concerns support the effect of culture on privacy attitudes to some extent. In a study comparing 38 countries, Bellman et al. (2004) investigated the influence of cultural values on individuals' concerns about different dimensions of privacy. Although they found some impact of cultural values on specific aspects of privacy concerns, they could not find an overall impact (Bellman et al., 2004).

3. Methodology

We propose a conceptual framework of DP and DS that takes the different perspectives into account, as is shown in Fig. 1. The framework makes a clear distinction between data protection, which represents the *legal perspective* and data security, which refers to the *technical perspective.* Both perspectives are very complex and a strict terminological distinction of the two perspectives contributes to a more structured discourse on DP and DS, as the terms are often used synonymously in both research and practice. In addition to these two perspectives, which are initiated or regulated by the state, we argue that there is another perspective that focuses on the subjects of DP and DS, namely the citizens. This *subjective perspective* represents the third perspective on DP and DS.

In addition to the conceptual framework, Fig. 1 illustrates the research design of the study. The empirical analysis represents a mixed-methods design, consisting of a media analysis and an online survey. The media analysis served as a foundation for the investigation of the subjective perspective and had two objectives. On the one hand, it was to examine to what extent and in which context the topic of DP and DS receives attention in public discourse. The examination of newspaper articles helped to determine how DP and DS are presented in public discourse. On the other hand, the media analysis provided a basis for the operationalisation of parts of the questionnaire. Specifically, the media analysis was used to collect technical terms that were referred to in connection with DP and DS. Based on the findings, an assessment of citizens' knowledge and understanding of DP and DS and related terms was then carried out by means of the quantitative online survey.

Venkatesh et al. (2013, 2016) specify different reasons for applying mixed-methods design approaches. In this case, the design was chosen for reasons of "completeness, development, expansion and diversity" (Venkateshet al., 2013, p. 26). Through the integration of the two methods, a more "complete" picture can be gained, as both the representation of DP and DS in the media as well as from an individual point of view are taken into consideration (Venkateshet al., 2016, p. 442). As the results of the media analysis are taken into account in the survey creation, "development" and "expansion" reasons are also of importance (Venkateshet al., 2016, p. 442). These results provided knowledge that was then further explored in the survey. Finally, "diversity" reasons play a role as both the media's and the citizens'perspectives in regard to DP and DS are considered (Venkateshet al., 2016, p. 442). In the following, first the media analysis will be outlined (section 3.1), followed by the main empirical part of this article, namely a survey among UK and German citizens (section 3.2).

3.1. Media analysis: data protection and data security in the public discourse

One way to obtain evidence of the public understanding of DP and DS is by analysing media coverage, since the media serve as a means of transportation of information and shape public opinion (Gunther, 1998). When investigating the public discourse, the media play a particularly important role. Accordingly, "[c]itizens organize their thoughts about issues through relevant discourse" (Hoffman & Slater, 2007, p. 59). Public discourse, however, is often not presented to citizens by political elites without any bias, but through different frames (Brewer, 2001).

Miller and Krosnick (2000, p. 301) summarise the research of media impact on the public by concluding that "media do indeed shape public opinion". Research on political communication assumes that public opinion is influenced by the way in which public debates frame issues and thus influence public perception of an issue, so that citizens "rely heavily on a 'media-constructed' version of reality" (Callaghan & Schnell, 2001, p. 184). It can therefore be assumed that focusing on specific aspects in the media also applies to the context of DP and DS. Furthermore, recent media coverage of the subject (e.g., in the context of GDPR implementation) has raised public awareness about DP and DS (Rohunen& Markkula, 2019).

In order to investigate the media framing of DP and DS for the purpose of this study, a content analysis of daily newspapers was conducted. This analysis also served as an empirical basis for the questions of the survey. Articles of two German and two UK newspapers were examined, of which one was more conservative (*The Times* and *Die Welt*) and one more liberal (*The Guardian* and *Die Süddeutsche*).

The periods for the media analysis were three different weeks between 2018 and 2019. Those were chosen on the basis of two particular political events relating to DP and DS in order to ensure the greatest possible coverage of DP and DS. In addition, an investigation period was chosen as a control period, which lay between the other two investigation periods that were linked to political events. The first week analysed was one week before the important data-protection-related EU events involving the decision concerning copyright reform. The second period of the media analysis was one week before the entry into force of the General Data Protection Regulation (GDPR). The information tool *Factiva* was used to search for articles containing either the term 'data

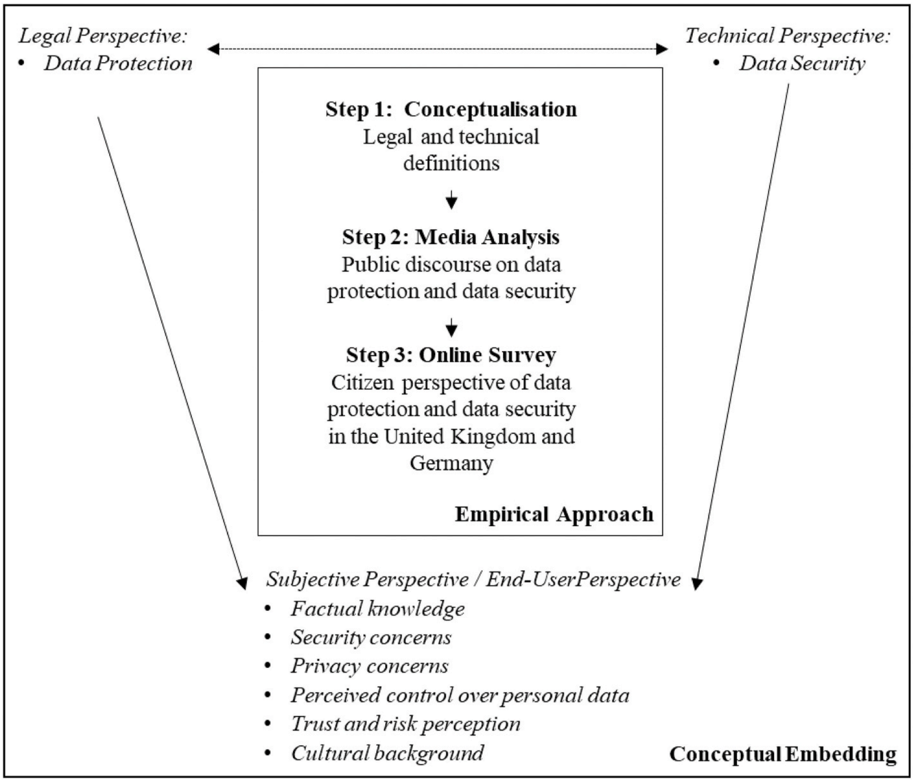
Legal Perspective:
• Data Protection
Technical Perspective:
• Data Security
Step 1: Conceptualisation
Legal and technical definitions
Step 2: Media Analysis
Public discourse on data protection and data security
Step 3: Online Survey
Citizen perspective of data protection and data security in the United Kingdom and Germany
Empirical Approach
Subjective Perspective / End-UserPerspective
• Factual knowledge
• Security concerns
• Privacy concerns
• Perceived control over personal data
• Trust and risk perception
• Cultural background
Conceptual Embedding

Fig. 1. Overview of the research design and conceptual embedding of the article.
Notes: The outer area represents the conceptual framework on three perspectives on DP and DS. The legal and the technical perspective are indirectly linked to each other, as they both manifest themselves in legislation, which is represented by the dotted line. As the legal and the technical perspectives are more present in the public discourse, they both directly influence the subjective perspective. This impact is represented by the solid line. The inner area constitutes the mixed-methods study design.

protection' or 'data security'.[2] After removing duplicates, a total of 128 articles were coded, of which 71% were articles from UK newspapers and 21% articles from German newspapers. It follows that the subject of DP and DS is receiving more attention in UK newspapers in quantitative terms. In addition to descriptive characteristics such as date and title, content-related variables capturing the way in which and by whom DP and DS was addressed, were coded.

3.2. *Survey design*

3.2.1. *Procedure and method*

The quantitative survey is based on an anonymous, cross-sectional online-survey that was distributed electronically among German and UK respondents. The online questionnaire was programmed using the online survey software *Qualtrics*. *Qualtrics* recruited the sample, and the data was collected during two weeks in July 2019.

3.2.2. *Survey instrument and questionnaire*

In total, the questionnaire consisted of 31 questions, including both closed and open-ended questions. Respondents were asked the question, in a broad sense, what they understand by DP and DS. In a narrower sense, the survey concept of investigating citizen perception of DP and DS was derived from literature exploring DP and DS from a theoretical, technical and legal perspective as well as from findings related to the individual concerns and priorities of online users. The questions can be assigned to five thematic blocks, dealing first with the definition of the concepts DP and DS and, second, associated terms and their relevance. The third block addressed respondents' familiarity with technical terms referred to in the media in connection with DP and DS. The fourth block covered concerns and risk perceptions towards DP and DS. The last block contained questions addressing control variables and socio-demographic characteristics (such as digital affinity, trust in the government and organisations, and the importance of data security and protection). The questions of the questionnaire in the form of variables together with the corresponding summary statistics are presented in Appendix Table A1. The questions were partly derived from literature and partly from the prior analysis of newspaper articles. The average duration to complete the survey was 7.22 min (S.D. = 2.94, N = 1,000).

3.2.3. *Participants*

The target population of respondents were UK and German citizens. These countries were chosen for this study due to the reasons outlined below. Both are large European countries in terms of population, with a population of around 83 million in Germany and around 67 million in the UK in 2020 (Eurostat, 2020). In both countries, the percentage of people who have never been online in 2019 is quite low in comparison with the EU average (Germany: 5%, UK: 3%, EU average: 9%) (DESI, 2020). Moreover, the majority of households in both countries (UK: 94%, Germany: 88%) have the possibility to connect to the internet via a fixed broadband connection (DESI, 2020). Furthermore, these countries generally display similar response styles in surveys (Harzing, 2006; Johnson et al., 2005; van Herk et al., 2004). They thus display similarities when it comes to geography, population, internet access and usage as well as similar survey response styles. Despite these similarities, there are important differences between the UK and Germany, especially when it comes to e-government, which is of particular interest for this study. In the UK, 89% of the population uses e-government services, whereas in Germany this share is considerably lower, with only 49% of the population using these services. This combination of comparable attributes but also remarkable differences in the use of e-government makes these two countries suited for a comparative study in the context of DP and DS from a subjective perspective against the background of e-government initiatives.

The questionnaire did not ask respondents for their nationalities as the decisive factor was the country of residence. The survey contained screening questions for the variables 'country of residence', 'age' and 'gender' to ensure a representative dataset for these variables per

[2] In German the search terms were 'Datenschutz' and 'Datensicherheit'.

country. After data cleansing, the final data set consisted of 1,000 individual responses.[3]

4. Results

4.1. Media analysis

To find out more about the attention DP and DS received in the media, a closer look at the coding results of the media analysis revealed that 57% of the articles dealt mainly with DP or DS, while 43% dealt only marginally with the issue (N = 128). When comparing newspapers from the UK and Germany by running a chi-square test, no significant differences between the priority of DP and DS within the articles could be found ($X^2 = 3.181$, N = 124, $p = .075$).

The article coding also revealed that 34% tackled the issue from a technical perspective, 60% from a legal perspective and 6% from a citizen (subjective) perspective (N = 199, multiple perspectives per article were possible). Newspapers from the UK and Germany addressed DP and DS with the same amount of 34% from a technical perspective, while only 1% of UK newspaper articles focussed on the subjective perspective as compared to 15% of German newspaper articles. DP and DS was tackled from a legal perspective by 65% of UK articles and 50% of German articles. In line with the lack of a definition of DP and DS in research, findings of the media analysis revealed that only one of 128 articles dealing directly or indirectly with this issue contained a definition.

The media analysis further served to collect technical terms that were referred to in connection with DP and DS.[4] These terms, along with theory-driven considerations, served as the basis for the development of the questionnaire. Respondents were later asked to rate their familiarity with these terms as presented in section 4.5.

4.2. Respondent characteristics

The sample consisted of 50% German and 50% UK respondents (N = 1,000).[5] The sample was weighted for a representative distribution concerning the age and sex of respondents based on the Eurostat distribution for the countries (see Eurostat, 2019). Accordingly, the sample is composed of 51% women and 49% men. Concerning the age distribution, only respondents who were at least 18 years old were included into the dataset. 11% of the respondents were between 18 and 24, 18% between 25 and 34, 32% between 35 and 49, 22% between 50 and 64 and 18% older than 64 years (N = 1,000).

4.3. Definition of data protection and data security

In order to investigate the underlying hypothesis that the public does not differentiate adequately between the terms DP and DS, respondents were directly asked in the beginning of the survey whether there was a difference between data protection and data security. In total 59% claimed that there was a difference between these terms, while 19% believed there was no difference and 22% responded to the question with “don’t know” (N = 1,000). Those who believed that there was a difference between those two terms were then asked, in an open-ended question, what they considered to be the biggest difference between data protection and data security.

With the aim of assessing respondents’ conceptualisation of the terms DP and DS, the answers to the open-ended question asking for the difference between DP and DS were coded based on their degree of correctness. As shown in Table 1, the coding of the responses was based on a distinction of six different categories of correctness: First, missing or invalid response, second, responses that were topic-related, but incorrect, third, correct answers for the concept of data protection only, fourth, correct answers for data security only and two separate categories for correct answers. Accordingly, the fifth category comprises responses that were correct but very generic while the sixth category captures fully correct answers. The quality and scope of the responses varied widely. While some responses did not contain any clarification or did not make sense (e.g., “nothing”, “not sure”, “good”), some answers were very detailed and sophisticated.

An example of a valid definition is the following response: “Data protection is the prevention of data disclosure through assurances and laws. Data security is the prevention of criminal attempts to gain access to data; protection against unauthorized access.” A shorter, but equally valid, explanation given by a respondent was the distinction that “data security is about technical measures to protect data. Data protection is about legal regulations for protection.” However, several responses to the question regarding the difference between DP and DS were incorrect or reflected an opinion rather than an objective definition, such as “[d] ata security comes across to me more unsafe than data protection.”

The coding results show that the most frequent response was topic-related, but incorrect. Accordingly, 41% of the 589 respondents who believed that there was a difference between the two terms provided responses addressing the biggest differences between these terms which were simply wrong or meaningless. Examples of responses of each category are presented in Table 1. One fifth of the respondents that had stated that there was a difference between the terms, were unable to specify this difference, answering the follow-up question with “unsure”, “not sure” or “I don’t know”. 13% were able to provide a correct but

Table 1
Coding results on differences between DP and DS.

Degree of correct responses	Percent (N)	Examples
Missing or invalid response	20% (117)	“Unsure”, “not sure” “I don’t know”
Topic-related, but incorrect	41% (244)	“Security protection is more reliable and hopefully better.” “Data security is working on security; protection is actively protecting.”
Correct answers for data protection only	10% (61)	“Data protection are regulations data security is different.” “There is no such thing as data security. Data protection defines what is legally possible.”
Correct answers for data security only	9% (53)	“Data security includes technical measures that serve to protect all possible data.” “Data security is a system which protects your IT networks whilst data protection is more related to communication processes.”
Nearly correct answers (generic)	13% (79)	“Data security relates more to the security of stored data; data protection relates more to the disclosure of data.” “Data security is if your data can be hacked by third parties. Data protection is if your data can be used for purposes you don’t approve of.”
Fully correct answers (correct)	6% (35)	“Data protection is the prevention of unauthorized access or disclosure through assurances and laws. Data security is the prevention of criminal attempts to gain access to data. Secured against unauthorized access.” “Data security means that data is technically secure (stored). Data protection means that there are regulations that protect data.”

Note: The coding is based on the responses to the open-ended question “What do you consider the biggest difference between ‘data security’ and ‘data protection’“, N = 589.

[3] Overall, more respondents participated in the survey, but incomplete responses and responses that took less time to finish than a third below the median were removed from the sample. 1,000 represents the number of individual responses contained in the cleansed data set.

[4] The identified terms are shown in Table 3.

[5] The terms ’German’ and ’UK’ refer to respondents’ country of residence.

rather generic or superficial distinction of both terms, while some respondents explained only one of the terms correctly (10% for 'data protection' and 9% for 'data security'). A fully correct and detailed distinction was offered by 6% of the respondents.

In many cases where a distinction was missing, the disclosure of data to third parties was mentioned. The responses to the open-ended question suggest that the transfer of data to third parties is central to the concept of DP and DS. Examples of this kind of responses include the following: "Data protection: I protect my data from unauthorized access," "Data protection, e.g., protect personal data from unauthorized access" and "[Data] protection is that you don't give it [data] to third parties."

The answers also repeatedly reflected an understanding that the two terms are in a causal relationship to each other. One respondent remarked that "data should be secure if you protect it." The responses to the open-ended questions suggest that a citizen's conceptualisation of DP and DS is predominantly based on the active transfer of data to third parties or the passive exploitation of data by third parties.

With the intention of capturing citizens' conception of DP and DS in more depth, respondents were asked to provide three keywords related to the terms.[6] In a first step, those responses which contained three keywords related to DP and DS were counted. Accordingly, 55% of the responses contained three keywords that were related to DP and DS as opposed to 46% providing fewer than three valid keywords (N = 1,000). In a next step, the first keywords given were coded by assigning the responses to different categories, which are shown in Fig. 2. 19% of the responses given were invalid responses such as "don't know" or "none." With regard to topic-related keywords, the most frequent answers were keywords related to the categories "Security" (19%), "Privacy" (14%) and "Cybercrime" (9%) (see Fig. 2).

The open associations with DP and DS reflect the concerns of respondents, as many key words fell into the categories "security," "privacy," "cybercrime," "protection" and "misuse." Together with the associations summed up under the category "individual preventive measures", these terms represent the subjective perspective. In addition, the results of the open associations indicate that the differentiation between the terms is often not clear or easy for citizens to explain as almost one fifth of the respondents provided an invalid response. In general, the results indicate that knowledge about DP and DS is limited, although a small number of respondents seem to be well-informed about both terms. Findings suggest that citizens associate concerns with the subjective perspective when thinking of DP and DS.

4.4. *Three perspectives on data protection and data security*

In order to examine to what extent citizens' understanding coincides with the technical and legal perspective of the terms, respondents were presented a list of nine terms and asked to choose the three terms that they most strongly associate with DP and DS. The nine terms were presented in a randomised order. Each term belongs to one of the three perspectives (three terms for each perspective). The results are shown in Table 2. Overall the largest frequency was found for the term 'personal data', which was chosen by 62% of respondents as one of the three words they associate most strongly with DP and DS, followed by 'right to privacy', which was selected by 54% of respondents. The weakest association was found for 'data privatisation', which was chosen by 9% of the respondents.

When calculating the percentage distribution of association per perspective, findings revealed that half of the selected keywords (50%, n = 1,398) belonged to the subjective perspective. 30% (n = 840) of the selected keywords can be assigned to the legal perspective and one fifth (20%, n = 576) to the technical perspective (N = 2,814). These findings underline the assumption that a subjective perspective exists in the context of DP and DS.

4.5. *Familiarity with data protection and data security*

To shed light on respondents' degree of familiarity with DP and DS, they were presented with related terms and aspects of DP and DS. To be more precise, terms were chosen that represent an operationalisation of the technical and legal perspectives, and respondents were asked if they associated those terms with DP and DS. The terms were derived from existing legislation, such as the GDPR. All terms were, therefore, related to DP and DS. The findings indicate that although some technical terms were associated with DP and DS, these revealed a much lower degree of association. Accordingly, 'Compliance with the General Data Protection Regulation (GDPR)' represents the aspect that was most frequently associated with DP and DS (82%). In contrast, only 55% and 56% of respondents said they associated the terms 'data recoverability' and 'storage of data in your home country' with DP and DS (N = 1,000 per term). This differing degree of association hints at a diverging understanding among the citizens of different countries concerning DP and DS from the legal and technical perspectives.

To examine citizens' familiarity with terminology used in the media, respondents were asked to indicate their degree of familiarity with several technical terms. In that question, the term 'familiarity' was defined as follows: "'Not familiar at all' means that you have never heard the term before and 'very familiar' means that you could explain the term." As shown in Table 3, results revealed a wide range of familiarity with terms used in newspapers. While terms such as 'spam email' and 'apps' show a rather strong familiarity (M = 4.14, *S. D.* = 0.98, N = 977; M = 4.00, *S.D.* = 1.02, N = 972), 16 terms scored mean values of between 3.5 and 3.9, indicating medium to rather high knowledge of their definition, and six terms were found to be less known, with values of between 3.0 and 3.4, indicating a medium level of familiarity. Respondents reported to be the least familiar with the terms 'log files' and 'blockchain' (M = 2.83, *S.D.* = 1.36, N = 910; M = 2.39, *S.D.* = 1.35, N = 910). In line with the results from the previous question, findings suggest some extent of knowledge and familiarity with terms used in connection with DP and DS. Differences in familiarity can however be detected between the different terms.

Participants were further asked to rank the importance of DP and DS for different services in order to examine whether the importance differs between services that deal with different types of personal information. The results indicate differences in the relevance of DP and DS depending on the type of service (Table 4). Accordingly, online banking represents the service in which DP and DS are considered to be of the highest importance. 88% of respondents rated DP and DS as "very important" for online banking (N = 983). In contrast, only 31% of respondents stated that DP and DS was very important for "Wiki platforms" (N = 920). Overall, findings indicate that the more private data a service requires, the greater the importance of data security and protection (Table 4).[7]

4.6. *Differences between the UK and Germany*

To investigate whether the results from the UK and German samples differed, they were subsequently compared to each other. To be able to

[6] A distinction between the terms was no longer made for the remaining part of the questionnaire. This was explained to respondents after the first question.

[7] A multiple regression was also run to investigate whether the familiarity with the terms in Table 3 could significantly predict the importance that data security and data protection are ensured when using the internet (F(26, 804) = 3.341, $R^2 = 0.10$, p = .000). The results indicate that three of 26 technical terms significantly predicted the importance to ensure data protection and security. Accordingly, familiarity with the GDPR (β = 0.11, *p* = .017) and hacking (β = 0.15, *p* = .014) was found to positively impact the data protection and security importance whereas a familiarity with Blockchain (β = −0.11, *p* = .021.) was found to decrease it.

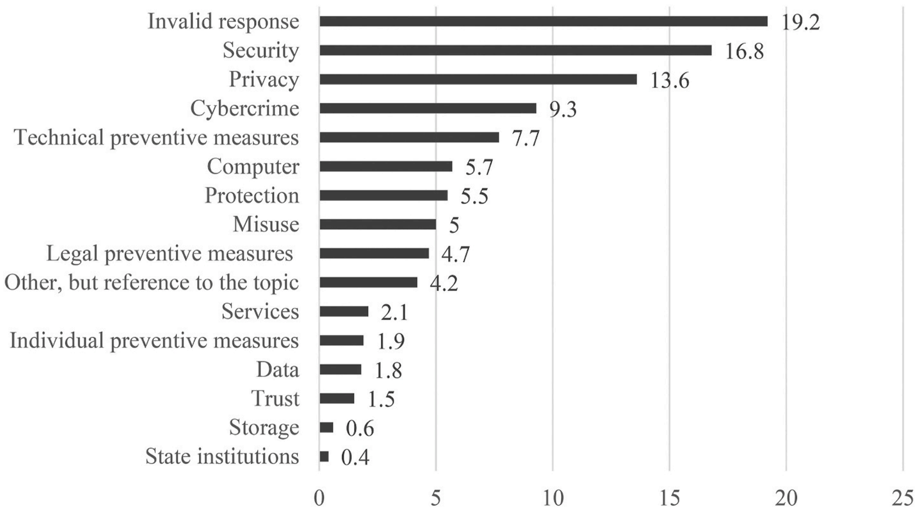

Fig. 2. Coding results for keywords associated with DP and DS.
Note: Bars represent percentages. The question was "'Data security' and 'data protection' are broad concepts. In general: What keywords come to mind when you think about 'data security' and 'data protection'?" (N = 1000).

Table 2
Three perspectives and their association with data protection and data security.

Perspective	Term	Percentage	Frequency	Total N
Legal perspective	Data protection guidelines	46	461	1000
	Data ownership	24	238	1000
	Data protection officer	14	141	1000
Technical perspective	Big data analysis	5	45	1000
	Data privatisation	9	90	1000
	Storage of data	44	441	1000
Subjective perspective	Right to privacy	54	544	1000
	Personal data	62	615	1000
	Data control	24	239	1000

Note: The percentages reflect the selection rate of the respective terms. As each participant could choose three terms, the absolute frequencies of each term are also represented in a separate column.

measure the overall level of concern, respondents were asked to grade their concerns about disclosing personal information on the internet by means of a ten-point scale (ranging from 1 = no concerns at all to 10 = very serious concerns). Results yielded a difference between the UK and German average levels of concern: UK respondents (M = 7.34, N = 500) were shown to have a significantly higher average concern to disclose personal data on the internet than their German counterparts (M = 7.09, N = 500), (t(998) = −2.037, *p* = .042). In contrast, no significant differences could be found for the average importance of a guarantee of DP and DS. When asked to rate how important it is to ensure DP and DS when using the internet, the average importance among the UK (M = 8.69) and German (M = 8.51, N = 1,000) sample were both high (t(998) = −1.673, *p* = .095). The results thus suggest that UK citizens show higher concerns than German citizens do, while both emphasise the importance of guaranteeing DP and DS.

Interestingly, trust in government does not seem to differ between the two countries. Respondents were asked to indicate their level of trust using a scale of between 1 (= no trust in the government at all) and 10 (=

Table 3
Familiarity with data security- and protection-related terms used in the media.

Media terms	M	SD	N	Media terms	M	SD	N
Spam email	4.14	0.98	977	Data leaks	3.58	1.17	963
Apps	4.00	1.02	972	Data loss	3.58	1.15	962
Firewall	3.97	1.02	971	Artificial intelligence	3.58	1.13	965
Social media	3.92	1.15	976	Phishing	3.57	1.24	963
Databases	3.83	1.07	975	Smartphone tracking	3.34	1.27	959
Cybercrime	3.81	1.06	975	5G mobile network	3.32	1.23	958
Hacking	3.76	1.13	966	VPN	3.29	1.35	939
Data storage	3.70	1.08	968	Algorithms	3.23	1.28	939
Data encryption	3.67	1.10	969	Digital literacy	3.10	1.28	929
Cloud	3.67	1.18	965	Privacy filters	3.01	1.38	938
Data Protection Act	3.64	1.14	970	Log files	2.83	1.36	919
Data theft	3.63	1.13	967	Blockchain	2.39	1.35	910
Trojans	3.61	1.18	959				
GDPR	3.58	1.14	975				

Note: Agreement on a scale from 1 (= not at all familiar) to 5 (= very familiar). Familiarity was defined as follows: "'Not familiar at all' means that you have never heard the term before and 'very familiar' means that you could explain the term."

Table 4
Importance of DP and DS for services.

Services	M	SD	N
Online banking	4.81	0.59	983
Online shopping services (e.g., Amazon)	4.65	0.73	985
E-government services	4.49	0.91	864
Social media (e.g., Facebook, Instagram, Snapchat, Twitter)	4.21	1.13	958
Video platforms (e.g., YouTube)	3.78	1.12	938
Search engine (e.g., Google)	3.76	1.34	388
Wiki platforms (e.g., Wikipedia)	3.64	1.20	920

Note: Mean agreement based on a scale from 1 (= not at all important) to 5 (= very important).

full trust in the government). When conducting an independent *t*-test to compare the trust in government, there was no significant difference in the self-stated trust scores for UK (M = 5.73, N = 500) and German respondents (M = 5.59, N = 500), (t(998) = −0.887, *p* = .375).[8] In contrast, when asked to express their trust in private-sector companies on a similar scale, there was a significant difference between the trust in companies for UK and German respondents. Results suggest that UK citizens (M = 5.56, N = 500) have a higher trust in private companies compared to German citizens (M = 5.18, N = 500), (t(998) = -0.2.758, *p* = .006). In addition, when asked whose responsibility it should be to ensure DP and DS, UK (72%, N = 489) respondents significantly more often felt that it should be the government rather than national private-sector companies as opposed to German citizens (65%, N = 478) (X^2 (1, 967) = 5.055, *p* = .027).

To shed more light on the individual perspective, respondents were asked to rate their concerns in relation to aspects connected with DP and DS. Results show that the degree of concern varies according to potential threat and country of residence.

As shown in Table 5, UK respondents on the whole seem to have stronger concerns with regard to DP and DS compared to German participants. However, respondents of both countries report rather strong concerns in general with several average concern scores around 4.0 indicating serious concern (five average concern scores above 4.0 for the UK and four average concern scores above 4.0 for Germany, see Table 5). The biggest concerns in both countries were about ‘fraudulent use of data’, although the average concerns were significantly higher among UK (M = 4.45, N = 495) than among German respondents (M = 4.33, N = 482), t(975) = −2.203, *p* = .028. The lowest degree of concern for both countries was found to be ‘restriction of freedom of expression and artistic freedom’ for which the mean level of concern also did not differ significantly between German and UK respondents. Concern regarding ‘data theft’ was found to be serious across both country samples, although the concern by UK subjects (M = 4.42, N = 492) was significantly stronger than that by German subjects (M = 4.26, N = 485), t (975) = −2.835, p = .005. Along similar lines, the findings revealed a significantly higher concern by UK participants towards the threats ‘identity theft’ (UK: M = 4.31, N = 495; Germans: M = 3.96, N = 480, t (973) = −5.688, *p* = .000), ‘companies exploiting my data for profit’ (UK: M = 4.22, N = 486; German: M = 4.06, N = 473, t(957) = −2.654, *p* = .008) and ‘electronic manipulation of elections’ (UK: M = 3.63, N = 482, German: M = 3.34, N = 470, t(950) = −3.806, *p* = .000) (see Table 5).

Table 5
Average concern in relation to DP and DS divided by country of residence.

Concerns	UK			Germany		
	M	SD	N	M	SD	N
Fraudulent use of data	**4.45**	**0.82**	**495**	**4.33**	**0.90**	**482**
Data theft	**4.42**	**0.78**	**492**	**4.26**	**0.92**	**485**
Identity theft	**4.31**	**0.84**	**495**	**3.96**	**1.04**	**480**
Sale of personal data to third parties	4.29	0.87	493	4.29	0.88	483
Companies exploiting my data for profit	**4.22**	**0.90**	**486**	**4.06**	**0.98**	**473**
Excessive collection of data	3.78	1.01	489	3.87	1.03	467
Electronic manipulation of elections	**3.63**	**1.16**	**482**	**3.34**	**1.23**	**470**
Fake news	3.59	1.13	487	3.53	1.16	463
Restriction of freedom of expression and artistic freedom	3.49	1.14	483	3.38	1.18	476

Note: Based on a five-point scale of between 1 (= no concerns at all) and 5 (= very serious concerns); bold indicates that the 95% confidence interval does not contain zero (significant difference in the mean concern between the UK and German samples).

In order to validate the results concerning trust in government and private organisations as well as concerns towards data use, respondents were asked for their agreement to four statements, three of which were taken from Joinson et al. (2006, p. 335ff.) which are based on the *Westin privacy segmentation*[9]. One additional statement was added to examine trust in public organisations. The statements and the corresponding degree of agreement by country are shown in Table 6.

Comparing the answers of the respondents from both countries, the results yielded differences in level of agreement. As illustrated in Table 6, results revealed a significantly higher level of agreement among UK respondents to the statement that “most businesses handle the personal information they collect about consumers in a proper and confidential way” compared to German respondents *(*X^2 (1, 1000) = 42.189, *p* = .000). The same pattern was found for the other two statements: “most public institutions handle the personal information they collect about consumers in an appropriate and confidential manner” and “existing laws and organisational practices provide a reasonable level of protection for consumer privacy today.” Both statements were met with significantly more approval among UK respondents compared to German respondents (first statement: X^2 (1, 1000) = 15.684, *p* = .000;

Table 6
Agreement with Westin statements according to country.

Statements	Sample	
	UK	Germany
“Most businesses handle the personal information they collect about consumers in a proper and confidential way.”		
Agreement	73% (366)	53% (267)
Disagreement	27% (134)	47% (233)
Chi-square	42.189***	
“Most public institutions handle the personal information they collect about consumers in an appropriate and confidential manner.”		
Agreement	76% (382)	65% (325)
Disagreement	24% (118)	35% (175)
Chi-square	15.684***	
“Existing laws and organisational practices provide a reasonable level of protection for consumer privacy today.”		
Agreement	70% (348)	48% (239)
Disagreement	30% (152)	52% (261)
Chi-square	49.008***	
“Consumers have lost all control over how personal information is collected and used by companies.”		
Agreement	82% (409)	83% (413)
Disagreement	18% (91)	17% (87)
Chi-square	0.109	

Notes: Recoded scale based on disagree (=strongly disagree and somewhat disagree); agree (=strongly agree and somewhat agree), **p* ≤ .05, ***p* ≤ .01, ****p* ≤ .001, N = 1000 per statement.

[8] Even after recoding trust to a dichotomous variable and removing the middle option, results did not reveal any evidence of a significant relationship by running a chi-square test (X^2 = . 850, N = 849, *p* = .382).

[9] The Westin privacy segmentation is a “scheme for categorizing the different levels of privacy concerns” and a methodology to measure participants’ “general privacy attitudes” (Joinsonet al., 2006, p. 335f., see also,; Westin, 1968).

second statement: X^2 (1, 1000) = 49.008, p = .000). The only statement where no significant difference between the answers of respondents from the two countries of residence were found was that "[c]onsumers have lost all control over how personal information is collected and used by companies" (X^2 (1, 1000) = 0.109, p = .741); in fact, respondents from both countries agreed quite strongly (Table 6).

Respondents were asked to type their subjective associations of the terms DP and DS. When comparing the results for these open-ended responses from the UK and Germany samples, results revealed a high degree of similarity and two clear differences in responses. While 25% of the UK respondents provided a keyword related to 'security', 8% of German respondents indicated a security-related first keyword. Furthermore, when comparing the findings of the countries, 27% of the German and 11% of the UK respondents gave an invalid response. This higher degree of invalid responses might indicate a higher degree of familiarity with the topic among UK respondents compared to German respondents.

In line with this consideration is the finding that UK respondents rated their familiarity with data security- and protection-related terms used in the media higher than German respondents: When comparing the familiarity among the two countries, the average self-reporting was found to be significantly higher for UK citizens for 22 out of 26 technical terms, except for the four terms 'blockchain', 'trojans', 'digital literacy' and 'data loss' (see Table 3 for a list of all terms).

The difference in familiarity of the terms becomes evident by the example of the *Data Protection Act* (2018) (German equivalent: Bundesdatenschutzgesetz, 2017). Whereas only around 15% (N = 479) of German respondents reported feeling comfortable explaining the term, twice as many (37%, N = 491) of UK respondents stated being comfortable to do so. This suggests that data protection legislation in the UK is better known than the corresponding legislation in Germany.[10]

5. Discussion

As the citizens' perspective is more diffuse and less conceptualised, we assumed that it was underrepresented in the public arena. Indeed, the media analysis revealed the dominance of the legal and technical perspectives over the subjective perspective in the public discourse. Due to a lack of a clear distinction between DP and DS in the public discourse, it could therefore be assumed that a clear distinction is also missing within the subjective perspective.

The results indicate the existence of a subjective perspective on DP and DS among citizens that does indeed differ from the legal and technical perspectives. In contrast to the technical and legal perspectives that address specific regulations and factual criteria in the context of handling data, the subjective perspective seems to be characterised by diffuse concerns. Findings suggest that a majority of citizens feel as if they have lost control over how their personal information is collected and used by companies. These concern patterns point toward a similar direction as previous studies, which were able to identify the misuse of data as a major concern of users (e.g., Dogruel & Joeckel, 2019).

When looking closer into citizens' concerns about DP and DS, our findings confirm previous studies (e.g., Dutton & Blank, 2013; Pleger et al., 2020) in the sense that citizens' concerns are found to be high, in some cases exceeding those found in previous studies (see Joinson et al., 2006). People's privacy concerns influence their behaviour (Carter & McBride, 2010; Phelps et al., 2000). At the same time, individuals seem to be trading off their privacy for a relatively low reward, implying a contradiction between their high level of concern and their actual behaviour – the so-called *privacy paradox* (Distleret al., 2020; Gerber et al., 2018; Kokolakis, 2017; Norberg et al., 2007). Understanding citizens' behaviour as well as their concerns is of crucial importance for e-government (Kokolakis, 2017).

With regard to e-government, it is important for citizens to have an understanding of DP and DS, as research has shown that security experts often overestimate the knowledge about security among end-users and implement solutions accordingly (Acaret al., 2016). Previous studies have shown that information can reduce privacy concerns in users (see, e.g., Lin et al., 2012). The results of this study contribute to this by emphasising the importance of a basic understanding of the terms DP and DS as a prerequisite for understanding and adequately addressing user concerns. Media analysis has shown that many terms are used in discourse that the population does not understand. The public discourse, therefore, takes place without the actual target group. In addition, the state should meet the needs of its population. Various studies underline the subjective relevance of DP and DS (Bergström, 2015; Distler et al., 2020; Palen & Dourish, 2003; Pleger et al., 2020). In order to meet this need, however, the state must know exactly what degree of DP and DS is important for its citizens, which in turn is influenced by citizens' understanding. The state cannot know how to comply with the request, or what exactly it should implement, if it does not know what its citizens want, as there are no 'objective' values for DP and DS. In this respect, a clear distinction between DP and DS and the education of citizens regarding DP and DS are important, as concrete policies and laws are established during implementation.

We also examined the question whether there were differences in individuals' concerns regarding DP and DS as expressed by UK citizens compared to German citizens. The findings suggest that UK citizens feel a significantly higher level of concern than their German counterparts. This is surprising because prior studies have found Germans to exhibit the highest level of concern about a potential misuse of personal data compared to other EU citizens (Dogruel& Joeckel, 2019, p. 1768). One explanation for this might stem from national events entering public debate. For instance, revelations in the summer of 2013 of the US and UK governments engaging in large-scale surveillance of private citizens based on data gathered by or transmitted on behalf of private entities had the positive effect of pushing personal data protection to the forefront of public consciousness in the UK (Lynskey, 2014, p. 597).

Overall, results for the UK and German dataset thus indicate that there are national differences in the subjective perspective. This aspect is particularly important, as it can mean that the cultural context might influence the subjective perspective. Against this background, the findings from the media analysis are also noteworthy, since the media analysis did not provide any indications of systematic differences in DP and DS reporting between the UK and Germany. However, differences were found with regard to the scope of reporting, according to which significantly more articles from UK newspapers focus on DP and DS than German newspapers. It could therefore be that the amount of reporting influences the citizen perspective on DP and DS.

On the issue of trust, both citizens' trust in their government and in private-sector companies was explored. Interestingly, no evidence of a significant difference between the trust felt by UK and German citizens in government could be found. In contrast, trust in private-sector companies was found to be higher among UK than among German respondents. In other words, most citizens seem to think that their data is handled in an appropriate manner by public and private institutions, but trust is significantly higher among UK compared to German citizens.

These results are of special importance when it comes to e-government initiatives, such as e-voting, because trust is, among others, an important prerequisite for the acceptance of e-government or e-voting (Carter & Bélanger, 2005; Carter et al., 2016; Distler et al., 2019). From the point of view of the public sector, this is an important finding, as

[10] Differences in familiarity with terms used in the media may be for language reasons. A large number of terms used in the media are English technical terms without a German translation, such as "Virtual Private Network," "Phishing," or "Cloud." However, a higher degree of familiarity among UK respondents was also found for terms that have a German translation. For instance, while only 18% (N = 480) of German respondents claimed to be very familiar with the term 'data theft' (i.e., 'Datendiebstahl'), 34% (N = 487) of UK respondents indicated being very familiar with the term.

e-government solutions can only be successfully implemented if they are accepted by users. As Combe (2009, p. 397) argues, "effective public service delivery by means of ICT's is necessarily dependent on trust forming relationships between citizens and state". The findings of this study indicate that trust as one necessary condition for the success of e-government efforts, is sufficient. In this connection, another finding of interest is that the state is seen as being responsible for ensuring DP and DS. It is, therefore, all the more important that the state takes the concerns of its citizens seriously and that it is transparent in its information about DP and DS. Concerning the state's requirement to deliver transparent information to its citizens, a major issue has to be addressed: On the one hand, information must be appropriate to the target group to adequately address concerns; also, the public discourse must take this into account. On the other hand, transparency also requires the active involvement of the public. Given that citizens understand DP- and DS-related information, they need to be proactive in informing themselves. The findings of this study suggest, however, that not even the former is currently the case. Thus, citizens simply do not have the necessary knowledge of the complex issues of DP and DS to inform themselves sufficiently. Results show that the importance citizens attribute to DP and DS does not match their understanding. Despite the fact that they attach great importance to DP and DS and have crucial concerns, they rely on a simplified and distorted conception of DP and DS. While it is not a citizen's duty to be an expert in the field of DP and DS, and since privacy should be guaranteed by design (see, e.g. Mubarak et al., 2013), we argue that a better understanding of the concepts could enable citizens to better articulate their concerns regarding DP and DS. In such a way, they can play their part in securing that the subjective perspective is taken into sufficient consideration when it comes to the introduction of e-government solutions, for example.

For instance, it was found that users rarely read privacy policies or terms and conditions provided by data controllers (Custerset al., 2018, p. 240; Mubarak et al., 2013, p. 714). Derived from the findings of this study, we argue that one reason why citizens fail to actively contribute to gain transparency stems from the fact that the resources required for this are not available, namely a thorough understanding of the concepts DP and DS. Despite the differences between the two countries, results indicate an overall tendency, meaning a lack of a clear conceptualisation and distinction of the terms 'data protection' and 'data security' despite the fact that DP and DS are of great importance to the citizens of both countries.

As a result, it is vital for citizens to learn what DP and DS actually mean and what is implied in order to empower them to be more proactive and responsible. Undeniably, DP and DS are complex concepts, which makes it difficult for a state to inform its citizens in a satisfactory manner. For instance, regarding data protection, Custers et al. (2018, p. 240) claim, that "it is difficult to explain the complexity of data processing in clear and plain language; when trying to use simple explanations, the complexity is reduced in a way that may no longer adequately reflect the reality of data processing". At the same time, literature has emphasised the importance of information management for public administration practice. Lips et al. (2005, p. 2) point out that "quality information" represents a key feature of an effective risk and trust management, which, in turn, is substantively important for effective public administration as a whole.

In this regard, the findings of this study contribute to more effective information management in the context of e-government in several respects: Given the status quo of citizens' understanding of DP and DS, a discussion about information quality is pointless because an understanding of the concepts must first be *created*. If the state provides high-quality information aiming to create transparency, this will currently not reach its citizens due to their lack of knowledge of the underlying concepts. In turn, citizens might not behave in a way to support such government efforts. Therefore, in order to provide citizens with DP and DS related information effectively, their conceptualisation must be taken into account. Governments should put particular emphasis on citizens' concerns surrounding their data by providing adequate information without assuming that citizens are able to correctly describe DP and DS. One way to do this is through the provision of understandable privacy policy notices. Privacy policy notices are often not read or understood as a result of the difficult language used and their textual length (see e.g. Ebert et al., 2021; Steinfeld, 2016), leaving citizens largely unaware of the consequences of their consent. We encourage governments to enter into dialogue with citizens to better understand their subjective perspective in terms of DP and DS and to increase transparency regarding how their data is being used in a way that is understandable to them.

6. Conclusions

The aim of this study was to shed light on citizens' perspectives on the concepts of data protection (DP) and data security (DS) by means of a media analysis and an online survey of 1,000 UK and German citizens. In the context of greater e-government efforts and a continuous increase in ICT applications in the public sector, ensuring DP and DS for citizens plays a particularly crucial role. Citizens — intentionally or unintentionally — produce data continuously, and the state has a duty to safeguard the personal and sensitive data of its citizens. Despite this relevance, research has largely neglected the citizens' perspective. We propose a three-dimensional framework that allows to conceptually separate the citizens' perspective on DP and DS from the legal and technical perspectives discussed in the public discourse.

The findings of the online survey show that although citizens attach a high level of importance to DP and DS and are seriously concerned, they often lack a detailed knowledge or a deeper understanding of these concepts. The majority of citizens are unaware of the exact definition and the demarcation of the terms DP and DS. Based on the assumption that citizens' understanding of the terms is limited, this study further examined how familiar citizens are with the terminology used in the media in connection with DP and DS. Results to this aspect were mixed, indicating that the familiarity with some terms is rather high, while some terms are lesser known.

Taken together, although DP and DS are omnipresent in the public discourse, findings indicate that the public discourse currently does not succeed in reaching the actual target group of governmental aspirations in this context, namely the users.

This study contributes to the growing literature on digitisation processes in the public sector by moving the citizens' perspective into the spotlight. The results reveal an alarming discrepancy between the subjective perspective on DP and DS and the legal and technical perspective within the public discourse, which makes it difficult for the state to reach, inform and educate its citizens. Future research should acknowledge the existence of the subjective perspective and examine it in more depth to further reveal causes for its occurrence and how it can be influenced. Although the findings reveal similar trends for both the UK and the German samples, differences in concerns could be found that require more in-depth investigation. The citizen concept of DP and DS contributes to the discourse between politics, technology, and the public in the context of e-government initiatives and their requirements for DP and DS.

We propose focusing on the *subjective perspective* as a conceptual basis for targeting the citizens' perspective rather than the legal and technical perspectives. Findings of this study provide evidence of the existence of such a subjective perspective, which goes beyond citizens' concerns but also encompasses their priorities and conceptualisations of DP and DS. The subjective perspective should therefore be taken into account when it comes to building up citizens' knowledge on DP and DS. The findings are of practical relevance as they show that citizens' understanding of DP and DS could be improved. A more pronounced understanding of DP and DS by citizens can foster a mutual understanding between the state and its citizens. This, in turn, is a prerequisite for e-government efforts that should take the subjective perspective of citizens into consideration in an adequate manner.

Acknowledgments

We would like to thank Michelle Moonen and Simone Dietrich, and our thanks go to Dr. Yvonne Hegele for her valuable feedback on the first drafts.

Appendix

Table A1
Variables, summary statistics and operationalization

Variable	Summary Statistics	Operationalization
Importance of data security and data protection for *social media*	*Mean:* 4.21 S.D.: 1.13 Min.: 1, Max.: 5 (Total N: 958)	On a scale of 1 = not important at all to 5 = very important
Importance of data security and data protection for *online banking*	*Mean:* 4.81 S.D.: 0.59 Min.: 1, Max.: 5 (Total N: 983)	On a scale of 1 = not important at all to 5 = very important
Importance of data security and data protection for *video platforms (*e.g. *YouTube)*	*Mean:* 3.78 S.D.: 1.12 Min.: 1, Max.: 5 (Total N: 938)	On a scale of 1 = not important at all to 5 = very important
Importance of data security and data protection for *wiki platforms (*e.g. *Wikipedia)*	*Mean:* 3.64 S.D.: 1.20 Min.: 1, Max.: 5 (Total N: 920)	On a scale of 1 = not important at all to 5 = very important
Importance of data security and data protection for *online shopping services (*e.g. *Amazon)*	*Mean:* 4.65 S.D.: 0.73 Min.: 1, Max.: 5 (Total N: 985)	On a scale of 1 = not important at all to 5 = very important
Importance of data security and data protection for *e-Government services*	*Mean:* 4.49 S.D.: 0.91 Min.: 1, Max.: 5 (Total N: 864)	On a scale of 1 = not important at all to 5 = very important
Importance of data security and data protection for *search engine (*e.g. *Google)*	*Mean:* 4.07 S.D.: 0.99 Min.: 1, Max.: 5 (Total N: 964)	On a scale of 1 = not important at all to 5 = very important
Familiarity with the term *General Data Protection*	*Mean:* 3.58 S.D.: 1.14 Min.: 1, Max.: 5 (Total N: 975)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *phishing*	*Mean:* 3.57 S.D.: 1.24 Min.: 1, Max.: 5 (Total N: 963)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *cybercrime*	*Mean:* 3.81 S.D.: 1.06 Min.: 1, Max.: 5 (Total N: 975)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *databases*	*Mean:* 3.83 S.D.: 1.07 Min.: 1, Max.: 5 (Total N: 975)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *apps*	*Mean:* 4.00 S.D.: 1.02 Min.: 1, Max.: 5 (Total N: 972)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *data leaks*	*Mean:* 3.58 S.D.: 1.17 Min.: 1, Max.: 5 (Total N: 963)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *spam email*	*Mean:* 4.14 S.D.: 0.98 Min.: 1, Max.: 5 (Total N: 977)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *firewall*	*Mean:* 3.97 S.D.: 1.02 Min.: 1, Max.: 5 (Total N: 971)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *VPN*	*Mean:* 3.29 S.D.: 1.35 Min.: 1, Max.: 5 (Total N: 939)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *data encryption*	*Mean:* 3.67 S.D.: 1.10 Min.: 1, Max.: 5 (Total N: 969)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *cloud*	*Mean:* 3.67 S.D.: 1.18 Min.: 1, Max.: 5 (Total N: 965)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *Blockchain*	*Mean:* 2.39 S.D.: 1.35 Min.: 1, Max.: 5 (Total N: 910)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *hacking*		On a scale of 1 = not familiar at all to 5 = very familiar

(*continued on next page*)

(*continued*)

Variable	Summary Statistics	Operationalization
	Mean: 3.76 S.D.: 1.13 Min.: 1, Max.: 5 (Total N: 966)	
Familiarity with the term *algorithms*	*Mean:* 3.23 S.D.: 1.28 Min.: 1, Max.: 5 (Total N: 939)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *Artificial Intelligence*	*Mean:* 3.58 S.D.: 1.13 Min.: 1, Max.: 5 (Total N: 965)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *smartphone tracking*	*Mean:* 3.34 S.D.: 1.27 Min.: 1, Max.: 5 (Total N: 959)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *social media*	*Mean:* 3.92 S.D.: 1.15 Min.: 1, Max.: 5 (Total N: 976)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *5G mobile network*	*Mean:* 3.32 S.D.: 1.23 Min.: 1, Max.: 5 (Total N: 958)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *Data Protection Act*	*Mean:* 3.64 S.D.: 1.14 Min.: 1, Max.: 5 (Total N: 970)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *data storage*	*Mean:* 3.70 S.D.: 1.08 Min.: 1, Max.: 5 (Total N: 968)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term log *files*	*Mean:* 2.83 S.D.: 1.36 Min.: 1, Max.: 5 (Total N: 919)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *privacy filters*	*Mean:* 3.01 S.D.: 1.38 Min.: 1, Max.: 5 (Total N: 938)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *data theft*	*Mean:* 3.63 S.D.: 1.13 Min.: 1, Max.: 5 (Total N: 967)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *trojans*	*Mean:* 3.61 S.D.: 1.18 Min.: 1, Max.: 5 (Total N: 959)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *digital literacy*	*Mean:* 3.10 S.D.: 1.28 Min.: 1, Max.: 5 (Total N: 929)	On a scale of 1 = not familiar at all to 5 = very familiar
Familiarity with the term *data loss*	*Mean:* 3.58 S.D.: 1.16 Min.: 1, Max.: 5 (Total N: 962)	On a scale of 1 = not familiar at all to 5 = very familiar
General concern about disclosing personal data on the internet – *UK*	*Mean:* 7.34 S.D.: 1.97 Min.: 1, Max.: 10 (Total N: 500)	On a scale of 1 = no concerns at all to 10 = very serious concerns
General concern about disclosing personal data on the internet – *Germany*	*Mean:* 7.09 S.D.: 2.00 Min.: 1, Max.: 10 (Total N: 500)	On a scale of 1 = no concerns at all to 10 = very serious concerns
Main concerns in relation to data security and data protection – *Germany* *Identity theft*	*Mean:* 3.96 S.D.: 1.04 Min.: 1, Max.: 5 (Total N: 480)	On a scale of 1 = no concerns at all to 5 = very serious concerns
Main concerns in relation to data security and data protection – *Germany* *Electronic manipulation of elections*	*Mean:* 3.34 S.D.: 1.23 Min.: 1, Max.: 5 (Total N: 470)	On a scale of 1 = no concerns at all to 5 = very serious concerns
Main concerns in relation to data security and data protection – *Germany* *Restriction of freedom of expression an artistic freedom*	*Mean:* 3.38 S.D.: 1.18 Min.: 1, Max.: 5 (Total N: 476)	On a scale of 1 = no concerns at all to 5 = very serious concerns
Main concerns in relation to data security and data protection – *Germany* *Sale of personal data to third parties*	*Mean:* 4.29 S.D.: 0.88 Min.: 1, Max.: 5 (Total N: 483)	On a scale of 1 = no concerns at all to 5 = very serious concerns
Main concerns in relation to data security and data protection – *Germany* *Fraudulent use of data*	*Mean:* 4.33 S.D.: 0.90 Min.: 1, Max.: 5 (Total N: 482)	On a scale of 1 = no concerns at all to 5 = very serious concerns
Main concerns in relation to data security and data protection – *Germany* *Data theft*	*Mean:* 4.26 S.D.: 0.92 Min.: 1, Max.: 5 (Total N: 485)	On a scale of 1 = no concerns at all to 5 = very serious concerns
		On a scale of 1 = no concerns at all to 5 = very serious concerns

(*continued on next page*)

(*continued*)

Variable	Summary Statistics	Operationalization
Main concerns in relation to data security and data protection – *Germany* *Excessive collection of data*	*Mean:* 3.87 S.D.: 1.03 Min.: 1, Max.: 5 (Total N: 467)	
Main concerns in relation to data security and data protection – *Germany* *Companies exploiting my data for profit*	*Mean:* 4.06 S.D.: 0.98 Min.: 1, Max.: 5 (Total N: 473)	On a scale of 1 = no concerns at all to 5 = very serious concerns
Main concerns in relation to data security and data protection – *UK* *Identity theft*	*Mean:* 4.31 S.D.: 0.84 Min.: 1, Max.: 5 (Total N: 495)	On a scale of 1 = no concerns at all to 5 = very serious concerns
Main concerns in relation to data security and data protection – *UK* *Electronic manipulation of elections*	*Mean:* 3.63 S.D.: 1.16 Min.: 1, Max.: 5 (Total N: 482)	On a scale of 1 = no concerns at all to 5 = very serious concerns
Main concerns in relation to data security and data protection – *UK* *Restriction of freedom of expression and artistic freedom*	*Mean:* 3.49 S.D.: 1.14 Min.: 1, Max.: 5 (Total N: 483)	On a scale of 1 = no concerns at all to 5 = very serious concerns
Main concerns in relation to data security and data protection – *UK* *Sale of personal data to third parties*	*Mean:* 4.29 S.D.: 0.87 Min.: 1, Max.: 5 (Total N: 493)	On a scale of 1 = no concerns at all to 5 = very serious concerns
Main concerns in relation to data security and data protection – *UK* *Fraudulent use of data*	*Mean:* 4.45 S.D.: 0.82 Min.: 1, Max.: 5 (Total N: 495)	On a scale of 1 = no concerns at all to 5 = very serious concerns
Main concerns in relation to data security and data protection – *UK* *Data theft*	*Mean:* 4.42 S.D.: 0.78 Min.: 1, Max.: 5 (Total N: 492)	On a scale of 1 = no concerns at all to 5 = very serious concerns
Main concerns in relation to data security and data protection – *UK* *Fake news*	*Mean:* 3.59 S.D.: 1.13 Min.: 1, Max.: 5 (Total N: 487)	On a scale of 1 = no concerns at all to 5 = very serious concerns

Variable	Summary Statistics	Operationalization
Main concerns in relation to data security and data protection – *UK* *Excessive collection of data*	*Mean:* 3.78 S.D.: 1.01 Min.: 1, Max.: 5 (Total N: 489)	On a scale of 1 = no concerns at all to 5 = very serious concerns
Main concerns in relation to data security and data protection – *UK* *Companies exploiting my data for profit*	*Mean:* 4.22 S.D.: 0.90 Min.: 1, Max.: 5 (Total N: 486)	On a scale of 1 = no concerns at all to 5 = very serious concerns
Agreement – *Germany "Consumers have lost all control over how personal information is collected and used by companies"*	*Mean:* 2.08 S.D.: 0.70 Min.: 0, Max.: 3 (Total N: 500)	On a scale of 0 = strongly disagree to 3 = strongly agree
Agreement – *Germany "Most businesses handle the personal information they collect about consumers in a proper and confidential way"*	*Mean:* 1.49 S.D.: 0.70 Min.: 0, Max.: 3 (Total N: 500)	On a scale of 0 = strongly disagree to 3 = strongly agree
Agreement – *Germany "Most public institutions handle the personal information they collect about consumers in an appropriate and confidential manner"*	*Mean:* 1.67 S.D.: 0.71 Min.: 0, Max.: 3 (Total N: 500)	On a scale of 0 = strongly disagree to 3 = strongly agree
Agreement – *Germany "Existing laws and organisational practices provide a reasonable level of protection for consumer privacy today"*	*Mean:* 1.43 S.D.: 0.73 Min.: 0, Max.: 3 (Total N: 500)	On a scale of 0 = strongly disagree to 3 = strongly agree
Agreement – *UK "Consumers have lost all control over how personal information is collected and used by companies"*	*Mean:* 2.00 S.D.: 0.66 Min.: 0, Max.: 3 (Total N: 500)	On a scale of 0 = strongly disagree to 3 = strongly agree
Agreement – *UK "Most businesses handle the personal information they collect about consumers in a proper and confidential way"*	*Mean:* 1.78 S.D.: 0.67 Min.: 0, Max.: 3 (Total N: 500)	On a scale of 0 = strongly disagree to 3 = strongly agree
Agreement – *UK* *"Most public institutions handle the personal information they collect about consumers in an appropriate and confidential manner"*	*Mean:* 1.86 S.D.: 0.68 Min.: 0, Max.: 3 (Total N: 500)	On a scale of 0 = strongly disagree to 3 = strongly agree
Agreement – *UK "Existing laws and organisational practices provide a reasonable level of protection for consumer privacy today"*	*Mean:* 1.75 S.D.: 0.69 Min.: 0, Max.: 3 (Total N: 500)	On a scale of 0 = strongly disagree to 3 = strongly agree
Relevance to ensure DPDS – *Germany*	*Mean:* 8.51 S.D.: 1.76 Min.: 1, Max.: 10 (Total N: 1000)	On a scale of 1 = not at all important to 10 = very important
Relevance to ensure DPDS – *UK*	*Mean:* 8.69 S.D.: 1.64 Min.: 1, Max.: 10 (Total N: 1000)	On a scale of 1 = not at all important to 10 = very important
Responsibility to ensure DPDS – *Germany*	*Share* (N = 478) The government: 65% (311) National private-sector companies: 35% (167)	Entities: 1 = The government 2 = National private-sector companies

Variable	Summary Statistics	Operationalization
Responsibility to ensure DPDS – *UK*	*Share* (N = 489) The government: 72% (351) National private-sector companies: 28% (138)	Entities: 1 = The government 2 = National private-sector companies
Responsibility company to ensure DPDS *Germany*	*Share* (N = 167) National private-sector companies: 21.6% (36) International private-sector companies: 11.4% (19) Both: 67.1% (112)	Entities: 1 = National private-sector companies 2 = International private-sector companies 3 = Both (i.e. national private-sector companies and international private-sector companies)
Responsibility company to ensure DPDS *UK*	*Share* (N = 137) National private-sector companies: 21.9% (30) International private-sector companies: 20.4% (28) Both: 57.7% (79)	Entities: 1 = National private-sector companies 2 = International private-sector companies 3 = Both (i.e. national private-sector companies and international private-sector companies)
Trust in government *Germany*	*Mean:* 5.59 S.D.: 2.38 Min.: 1, Max.: 10 (Total N: 500)	On a scale of 1 = no trust at all to 10 = full trust
Trust in government *UK*	*Mean:* 5.73 S.D.: 2.40 Min.: 1, Max.: 10 (Total N: 500)	On a scale of 1 = no trust at all to 10 = full trust
Trust in private sector companies – *Germany*	*Mean:* 5.18 S.D.: 2.18 Min.: 1, Max.: 10 (Total N: 500)	On a scale of 1 = no trust at all to 10 = full trust
Trust in private sector companies – *UK*	*Mean:* 5.56 S.D.: 2.20 Min.: 1, Max.: 10 (Total N: 500)	On a scale of 1 = no trust at all to 10 = full trust
Political orientation *Germany*	*Mean:* 5.02 S.D.: 1.77 Min.: 1, Max.: 10 (Total N: 500)	On a scale of 1 = far left to 10 = far right
Political orientation *UK*	*Mean:* 5.46 S.D.: 1.83 Min.: 1, Max.: 10 (Total N: 500)	On a scale of 1 = far left to 10 = far right

Variable	Summary Statistics	Operationalization
Education – *Germany*	*Share* (N = 500) No education: 1.4% (7) Secondary School: 3.4% (17) Vocational training: 39.0% (195) A Level or equivalent: 20.6% (103) University of applied sciences degree: 15.8% (79) University degree: 19.2% (96) Other: 0.6% (3)	Level of education: 1 = No education 2 = Secondary School 3 = Vocational training 4 = A Level or equivalent 5 = University of applied sciences degree 6 = University degree 7 = Other
Education – *UK*	*Share* (N = 500) No education: 1.2% (6) Secondary School: 19.2% (96) Vocational training: 8.4% (42) A Level or equivalent: 25.0% (125) University of applied sciences degree: 8.2% (41) University degree: 36.4% (182) Other: 1.6% (8)	Level of education: 1 = No education 2 = Secondary School 3 = Vocational training 4 = A Level or equivalent 5 = University of applied sciences degree 6 = University degree 7 = Other

Credit author statement

Lyn E. Pleger, Conceptualization, Investigation, Methodology, Formal analysis, Data curation, Visualization, Project administration, Writing – original draft, Supervision, Writing – review & editing. Katharina Guirguis: Conceptualization, Investigation, Methodology, Writing – original draft, Writing – review & editing. Alexander Mertes: Funding acquisition, Resources, Writing – review & editing.

References

Acar, Y., Fahl, S., & Mazurek, M. L. (2016). *You are not your developer, either: A research agenda for useable security and privacy research beyond end users* (pp. 3–8). IEEE Cybersecurity Development (SecDev), 2016.

Aïmeur, E., Brassard, G., & Rioux, J. (2013). Data privacy: An end-user perspective. *International Journal of Computer Networks and Communications Security, 1*(6), 237–250.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society, 20*(5), 313–324.

Bennett, C. J. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press.

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior, 53*, 419–426.

Brewer, P. R. (2001). Value words and lizard brains: Do citizens deliberate about appeals to their core values? *Political Psychology, 22*(1), 45–64.

Brodie, C., Karat, C.-M., Karat, J., & Feng, J. (2005). Useable security and privacy: A case study of developing privacy management tools. *Proceedings of the 2005 symposium on useable privacy and security - SOUPS '05*.

Brough, A. R., & Martin, K. D. (2019). Critical roles of knowledge and motivation in privacy research. *Current Opinion in Psychology*.

Bundesdatenschutzgesetz. (2017), 05.06.20 http://www.gesetze-im-internet.de/bdsg_2018/.

Callaghan, K., & Schnell, F. (2001). Assessing the democratic debate: How the news media frame elite policy discourse. *Political Communication, 18*(2), 183–213.

Carter, L., & Bélanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal, 15*(1), 5–25.

Carter, L., & McBride, A. (2010). Information privacy concerns and e-government: A research agenda. *Transforming Government: People, Process and Policy, 4*(1), 10–13.

Carter, L., Weerakkody, V., Phillips, B., & Dwivedi, Y. K. (2016). Citizen adoption of E-government services: Exploring citizen perceptions of online services in the United States and United Kingdom. *Information Systems Management, 33*(2), 124–140.

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly, 35*(3), 445–459. https://doi.org/10.1016/j.giq.2018.04.002

Combe, C. (2009). Observations on the UK transformational government strategy relative to citizen data sharing and privacy. *Transforming Government: People, Process and Policy, 3*(4), 394–405.

Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Report, 34*(2), 234–243. https://doi.org/10.1016/j.clsr.2017.09.001

Data Protection Act. (2018), 20.08.2019 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

DESI. (2020). *Digital economy and society index 2020*. https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi.

DiMase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions, 35*(2), 291–300.

Distler, V., Lallemand, C., & Koenig, V. (2020). How acceptable is this? How user experience factors can broaden our understanding of the acceptance of privacy trade-offs. *Computers in Human Behavior, 106*, 106227.

Distler, V., Zollinger, M.-L., Lallemand, C., Roenne, P. B., Ryan, P. Y. A., & Koenig, V. (2019). Security—visible, yet unseen? *Proceedings of the 2019 CHI Conference on human Factors in computing. Systems - CHI, '19*, 1–13.

Dogruel, L., & Joeckel, S. (2019). Risk perception and privacy regulation preferences from a cross-cultural perspective. A qualitative study among German and U.S. Smartphone users. *International Journal of Communication, 13*, 20.

Dutton, W. H., & Blank, G. (2013). *Cultures of the internet* (Vol. 64). The Internet in Britain.

Ebert, N., Ackermann, K. A., & Scheppler, B. (2021). Bolder is better: Raising user awareness through salient and concise privacy notices. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 16*.

Eurostat. (2019). https://ec.europa.eu/eurostat/home.

Eurostat. (2020). *Data Explorer. Population on 1 January by age group and sex*. https://appsso.eurostat.ec.europa.eu/.

Fischer, P., & Hofer, P. (2011). Datenschutz. In *Lexikon der Informatik (12.*. Springer.

Friedewald, M., Burgess, J. P., Čas, J., Bellanova, R., & Peissl, W. (Eds.). (2017). *Surveillance, privacy and security. Citizens' perspectives*. Routledge.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security, 77*, 226–261.

Goddard, Michelle (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research, 59*(6), 703–705.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users. *Information & Management, 20*(1), 13–27.

Gunther, Albert C. (1998). The persuasive press inference: Effects of mass media on perceived public opinion. *Communication Research, 25*(5), 486–504.

Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Report, 28*(3), 263–272.

Harzing, A.-W. (2006). Response styles in cross-national survey research: A 26-country study. *International Journal of Cross Cultural Management, 6*(2), 243–266.

van Herk, H., Poortinga, Y. H., & Verhallen, T. M. M. (2004). Response styles in rating scales: Evidence of method bias in data from six EU countries. *Journal of Cross-Cultural Psychology, 35*(3), 346–360.

Hoepman, J.-H. (2014). Privacy design strategies. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, & T. Sans (Eds.), *ICT systems security and privacy protection* (Vol. 428, pp. 446–459). Springer Berlin Heidelberg.

Hoffman, L. H., & Slater, M. D. (2007). Evaluating public discourse in newspaper opinion articles: Values-framing and integrative complexity in substance and health policy issues. *Journalism & Mass Communication Quarterly, 84*(1), 58–74.

Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions and organizations across Nations*. SAGE Publications.

John, B. (2018). Are you ready for general data protection regulation? *BMJ, 360*.

Johnson, T., Kulesa, P., Cho, Y. I., & Shavitt, S. (2005). The relation between culture and response styles: Evidence from 19 countries. *Journal of Cross-Cultural Psychology, 36*(2), 264–277.

Joinson, A. N., Paine, C., Buchanan, T., & Reips, U.-D. (2006). Watching me, watching you: Privacy attitudes and reactions to identity card implementation scenarios in the United Kingdom. *Journal of Information Science, 32*(4), 334–343.

Jozani, M., Ayaburi, E., Ko, M., & Choo, K.-K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior, 107*, 106260.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122–134.

Kokott, J., & Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law, 3*(4), 222–228.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering, 4*(3), 127–135.

Landwher, C. (2018). 2018: A big year for privacy. *Communications of the ACM, 62*(2), 20–22.

Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J. I., & Zhang, J. (2012). Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp, '12*, 501.

Lips, M., Taylor, J. A., & Bannister, F. (2005). Public administration in the information society: Essays on risk and trust. *Information Polity, 10*(1,2), 1–9.

Lynskey, O. (2014). Deconstucting data protection: The 'added-value'of a right to data protection in the EU legal order. *International and Comparative Law Quarterly, 63*(3), 569–597.

MacKenzie, Scott B., Podsakoff, Philip M., & Podsakoff, Nathan P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly, 35*(2), 293–334. https://doi.org/10.2307/23044045

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355.

Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues, 59*(2), 411–429.

Ma, L., & Zheng, Y. (2017). National e-government performance and citizen satisfaction: A multilevel analysis across European countries. *International Review of Administrative Sciences, 85*(3), 506–526.

Miller, J. M., & Krosnick, J. A. (2000). News media impact on the ingredients of presidential evaluations: Politically knowledgeable citizens are guided by a trusted source. *American Journal of Political Science, 44*(2), 301–315.

Mubarak, A. I., Zyngier, S., & Hodkinson, C. (2013). Privacy by design and customers' perceived privacy and security concerns in the success of e-commerce. *Journal of Enterprise Information Management, 26*(6), 702–718.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126.

van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of Consumer Policy, 42*(1), 91–107.

Ortlieb, M., & Garner, R. (2016). Sensitivity of personal data items in different online contexts. *IT - Information Technology, 58*(5).

Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. *NEW HORIZONS, 5*, 8.

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in computing* (5th ed.). Pearson Education.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy and Marketing, 19*(1), 27–41.

Phillips, D. J. (2004). Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies. *New Media & Society, 6*(6), 691–706.

Pleger, L. E., Mertes, A., Rey, A., & Brüesch, C. (2020). *Allowing users to pick and choose: A conjoint analysis of end-user preferences of public e-services*. Government Information Quarterly, 101473.

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies, 71*(12), 1133–1143.

Presthus, W., & Sørum, H. (2019). Consumer perspectives on information privacy following the implementation of the GDPR. *Go for It: Where IS Researchers Aren't Researching, 7*(3), 19–34.

Rainie, L., & Duggan, D. (2015). *Privacy and information sharing*. Pew Research Center. http://www.pewinternet.org/2016/01/14/2016/Privacy-and-Information-Sharing/.

Regulation. (2016). *679 of the European Parliament and of the Council—of 27 April 2016—on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. EU) 2016/679 of the European Parliament and of the Council. (n.d.). Regulation (EU).

Rempel, E., Barnett, J., & Durrant, H. (2019). Contrasting views of public engagement on local government data use in the UK. In *Proceedings of the 12th international conference on theory and practice of electronic governance - ICEGOV2019* (pp. 118–128).

Richter, P. (2012). Datenschutz durch Technik und die Grundverordnung der EU-Kommission. *Datenschutz und Datensicherheit - DuD, 36*(8), 576–580.

Rohunen, A., & Markkula, J. (2019). On the road – listening to data subjects' personal mobility data privacy concerns. *Behaviour & Information Technology, 38*(5), 486–502.

Romanou, A. (2018). The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Computer Law & Security Report, 34*(1), 99–110.

Roßnagel, A. (2007). *Datenschutz in einem informatisierten Alltag: Gutachten im Auftrag der Friedrich-Ebert-Stiftung*. Friedrich-Ebert-Stiftung.

Sheldon, K. M., Elliot, A. J., Kim, Y., & Kasser, T. (2001). What is satisfying about satisfying events? Testing 10 candidate psychological needs. *Journal of Personality and Social Psychology, 80*(2), 15.

Spiekermann, S. (2012). The challenges of privacy by design. *Communications of the ACM, 55*(7), 38–40.

Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K.-L. (2015). The challenges of personal data markets and privacy. *Electronic Markets, 25*(2), 161–167.

Steinfeld, N. (2016). "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. *Computers in Human Behavior, 55*, 992–1000. https://doi.org/10.1016/j.chb.2015.09.038

Tamò-Larrieux, A. (2019). Designing for privacy and its legal framework. *Data protection by design and default for the internet of things*. Springer.

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy, 38*(1), 1–22.

Tsavli, M., Efraimidis, P. S., Katos, V., & Mitrou, L. (2015). Reengineering the user: Privacy concerns about personal data on smartphones. *Information & Computer Security, 23*(4), 394–405.

United Nations. (2018). United Nations E-government survey 2018. Gearing E-government to support transformation towards sustainable and resilient societies. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018.

Venkatesh, V., Brown, S., University of Arizona, Sullivan, Y., State University of New York, & Binghamton. (2016). Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems, 17*(7), 435–494. https://doi.org/10.17705/1jais.00433

Venkatesh, V., Brown, S. A., University of Arizona Bala, H., & Indiana University.. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly, 37*(1), 21–54. https://doi.org/10.25300/MISQ/2013/37.1.02

Voigt, P., & von dem Bussche, A. (2017). *The EU general data protection regulation (GDPR). A practical guide*. Springer International Publishing.

Wagner, I., & Eckhoff, D. (2018). Technical privacy metrics: A systematic survey. *ACM Computing Surveys, 51*(3), 57.

Westin, A. (1968). *Privacy And Freedom. Washington and Lee Law Review, 25*(1), 166.

Widjaja, A. E., Chen, J. V., Sukoco, B. M., & Ha, Q.-A. (2019). Understanding users' willingness to put their personal information on the personal cloud-based storage applications: An empirical study. *Computers in Human Behavior, 91*, 167–185.

Wilkowska, W., & Ziefle, M. (2012). Privacy and data security in E-health: Requirements from the user's perspective. *Health Informatics Journal, 18*(3), 191–201.

Wolters, P. T. J. (2018). The control by and rights of the data subject under the GDPR. *Journal of Internet Law, 22*(1), 7–18.

Wolters, P. T. J. (2019). The enforcement by the data subject under the GDPR. *Journal of Internet Law, 22*(8), 22–31.

Wu, Y. (2014). Protecting personal data in E-government: A cross-country study. *Government Information Quarterly, 31*(1), 150–159.

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management, 56*(4), 570–601.

Zafar, H. (2013). Human resource information systems: Information security concerns for organizations. *Human Resource Management Review, 23*(1), 105–113.