University of Passau IRDG Research paper Series No. 22-14

Cultural Influences on Personal Data Disclosure Decisions

German Perspectives

Sarah Howe

May 2022

Place of Publication

Institute for Law of the Digital Society, University of Passau

c/o Chair of German and European Private Law, Civil Procedure, and Legal Theory

Innstraße 39, 94032 Passau

https://www.jura.uni-passau.de/irdg/

Author

Sarah Howe is a student research assistant at the University of Passau and part of an interdisciplinary research project that scrutinizes the disclosure of personal data in a legal, cultural studies and information systems context.

Abstract

The paper captures survey findings about factors that influence Germans' willingness to share (WTS) their personal data from a cultural studies point of view. It is part of a series of country reports that have been composed in the interdisciplinary research project *Vectors of data disclosure – a comparative study of the use of personal data from a legal, cultural studies, and information systems perspective*[1], funded by the Bavarian Research Institute for Digital Transformation[2]. This report puts a specific focus on facets of data protection literacy.

Cite as

Howe, S. (2022). Cultural Influences on Personal Data Disclosure Decisions – German Perspectives. *University of Passau Institute for Law of the Digital Society Research Paper Series No. 22-14.* https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/.

Keywords

Culture, Data Disclosure, Digitalization, Germany, Information Governance, Privacy, Willingness to Share (WTS) Data.

[1] Lead principal investigator: Moritz Hennemann, further principal investigators: Kai von Lewinski, Daniela Wawra, and Thomas Widjaja; external advisor: Urs Gasser.

[2] https://www.bidt.digital/ (last access: 11/24/2021).

Contents

I. Introduction ... 1

II. Selected Survey Data ... 2

III. Digital Competitiveness ... 2

IV. General Value of Informational Privacy ... 3

V. Degree of Privacy of Data ... 6

VI. Benefits Associated with Data Disclosure ... 8

VII. Privacy Concerns and Risks ... 9

1. Concerns and Risks related to Data Security ... 9

2. Concerns and Risks related to Data Control ... 9

VIII. Data Protection Literacy ... 10

IX. Attitudes Towards Data Receiver ... 15

1. Attitudes Towards Governments ... 15

2. Attitudes Towards Companies ... 17

X. Communication on Data Use ... 19

XI. Key Findings ... 20

1. Digital Competitiveness ... 20

2. General Value of Informational Privacy ... 20

3. Degree of Privacy of Data ... 21

4. Benefits Associated with Data Disclosure ... 21

5. Privacy Concerns and Risks ... 21

a. Data Security ... 21

b. Data Control ... 22

6. Data Protection Literacy ... 22

7. Attitudes Towards Data Receiver ... 23

a. Attitudes Towards Governments ... 23

b. Attitudes Towards Companies ... 23

8. Communication on Data Use ... 23

XII. References ... 23

I. Introduction[3]

This is one of several country reports that have been composed in our research project *Vectors of data disclosure – A comparative study of the use of personal data from a legal, cultural studies, and information systems perspective*[4], funded by the Bavarian Research Institute for Digital Transformation.[5] It focuses on cultural influences on people's willingness to share (WTS) personal data as expressed in surveys that reflect prevailing views, assumptions, attitudes, evaluations, and reported behaviors of German citizens in relation to data disclosure. As a first step in our research project, we concentrate on surveys to get a general picture of a culture's mentality with regard to data disclosure based on as broad a data base as possible. This provides us with insights into the cultural preconditions of information governance in Germany. Our approach can be characterized as a macro level analysis (cf. Wawra 2022). We have composed similar 'reports' for other countries in our project, since we are planning a cultural comparative study as a next research step. This has also led to the decision to rely primarily on extensive global surveys in our reports to facilitate the following country comparisons. Secondarily, we have integrated surveys that cover at least some of our study countries. Wawra (2022) is an introduction to our project from a cultural perspective, which provides background information on the research context and details the cultural research design. The paper also introduces the parameters along which all of our cultural reports are structured. The following parameters have been identified as central to capture the narrower cultural context of data disclosure decisions on a macro level (cf. Wawra 2022): Digital Competitiveness (section III.), General Value of Informational Privacy (IV.), Degree of Privacy of Data (V.), Benefits Associated with Data Disclosure (VI.), Privacy Concerns and Risks (VII.), Data Protection Literacy (VIII.), Attitudes towards Data Receiver (IX.), and Communication on Data Use (X.) (see Figure 1). Data Protection Laws is another parameter that is detailed in separate legal country reports. Depending on the specific situational context, the parameters can all potentially have more or less influence on people's willingness to share (WTS) personal data. Overall, the structure of the country reports that have been compiled in our project is the same. The descriptions of the individual parameters have been adopted from Wawra (2022) and are rendered in italics.

[3] by Daniela Wawra.

[4] Lead principal investigator: Moritz Hennemann; further principal investigators: Kai von Lewinski, Daniela Wawra, and Thomas Widjaja.

[5] https://www.bidt.digital/ (last access: 11/24/2021).

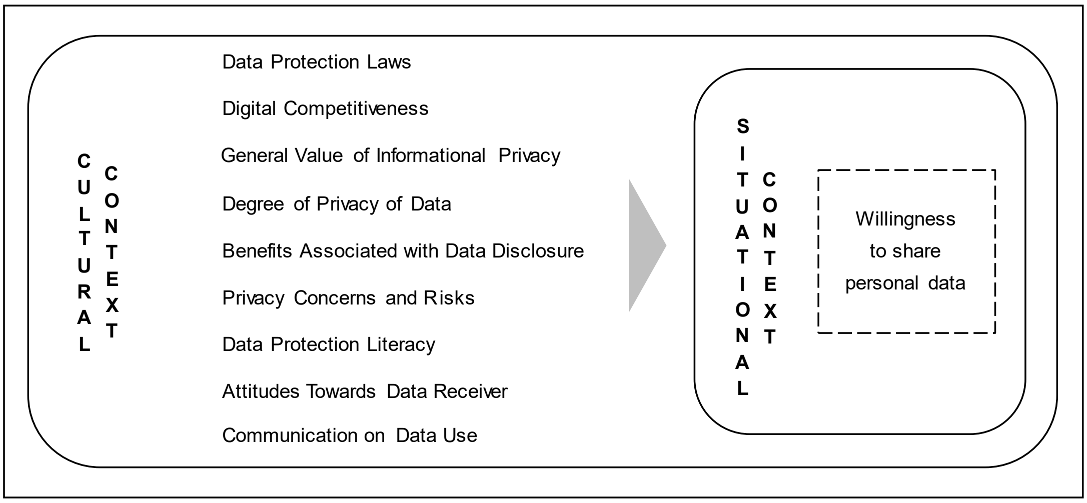
CULTURAL CONTEXT
Data Protection Laws
Digital Competitiveness
General Value of Informational Privacy
Degree of Privacy of Data
Benefits Associated with Data Disclosure
Privacy Concerns and Risks
Data Protection Literacy
Attitudes Towards Data Receiver
Communication on Data Use
SITUATIONAL CONTEXT
Willingness to share personal data

Fig. 1. Central parameters of data disclosure (from Wawra 2022)

II. Selected Survey Data

This report summarizes relevant results from major recent cross-national and national surveys and studies on informational privacy, data control, data protection, and data disclosure in Germany. Appendix 1 (adopted and adapted from Kessel 2022) gives an overview of the studies included and demographic details, i.e., countries of investigation, sample size, age of respondents, gender, education, socio-economic status, ethnicity, and political orientation. In regard to sample size, most included studies interrogated roughly 1000-2000 people. The study conducted by Trepte and Masur (2017) has by far the largest sample size with 3278 respondents. Moreover, the only included survey with a fairly small sample size is that by Kowalewski et al. (2015) with 110 participants.

III. Digital Competitiveness

[The parameter Digital Competitiveness] is understood in the sense of the "IMD World Digital Competitiveness Ranking" (WDCR), a well-established and widely accepted regularly published ranking, as the "capacity of economies to use digital technologies to transform themselves" (IMD 2021, p. 3). The WDCR "analyzes and ranks the extent to which countries adopt and explore digital technologies leading to transformation in government practices, business models and society in general" (IMD 2021, p. 32).[6] *Specifically, the WDCR aggregates scores to compare 64 countries in terms of 52 criteria relating to "knowledge", "technology", and "future readiness" (IMD 2021, p. 3, 32, 33). Knowledge describes the "[k]now-how necessary to discover, understand and build new technologies" (IMD 2021, p. 33) and is further divided into the subfactors of talent, training and education, as well as scientific concentration relating to, e.g., expenditure on research & development, and high-tech patent grants. The factor technology comprises the "[o]verall context that enables the development of digital technologies" (IMD 2021, p. 33), including the subfactors "regulatory framework", "capital", and "technological framework". Future readiness explains the "[l]evel of country preparedness to exploit digital transformation" (IMD 2021, p. 33) and measures*

[6] Wawra (2022, IV. 2.).

adaptive attitudes, business agility, and IT integration to rank the level of how countries are prepared for exploiting digital transformation (cf. IMD 2021, p. 33).[7]

In terms of the country's overall digital performance, Germany was ranked in 18th place out of 64 countries in 2021. Looking into factor rankings in 2021, Germany was ranked 14th for its state of **knowledge**, 31st in **technology** and 18th regarding **future readiness** for digitization. Analyzing Germany's overall rank from the past five years, it has deteriorated by one rank since 2017. Germany's knowledge has slightly decreased (from 13th in 2017 to 14th in 2021), while its digital technology has worsened (from 21st in 2017 to 31st in 2021) and its rank in the category future readiness in 2021 is the same again as in 2017 (18th rank in both years), after fluctuation in the years in between (cf. IMD 2021, p. 84).

Digital knowledge is divided into three subfactors: **talent, training and education, scientific concentration**. In regard to talent, Germany is positioned in 21st place while only in 54th place in digital and technological skills, which is one of the subfactor's items. Germany ended up 17th in training and education and 6th in scientific concentration (cf. IMD 2021, p. 85).

Subfactor rankings for Germany's **technology** position the country's **regulatory framework** in 25th place but 9th in intellectual property rights, which is an item of the subcategory. Additionally, Germany occupies the 23rd place in **capital** while only coming in 31st place in funding for technological development which is a subcategory of capital and 43rd place in **technological framework**.

Future readiness is divided into yet another three subcategories, one of which is **adaptive attitudes** where Germany ranks in 23rd position. In **business agility**, Germany is positioned in 15th place and in **IT integration** in 20th place. Looking at E-participation, Germany is in 45th rank and in smartphone possession in 23rd, both of which are subitems of the category adaptive attitudes. In the subcategory of business agility, Germany is positioned in 53rd place regarding the use of big data and analytics. Finally, in the subcategory of IT integration, E-government and Cyber security rank 24th (cf. IMD 2021, p. 85).

In conclusion, Germany's subfactor ranks for knowledge belong to the top third of the scale, with emphasis on the country's outstanding performance in scientific concentration (6th in rank). Technology subfactors, including regulatory framework and capital can be positioned in the overall higher midrange whilst the technological framework is in the bottom third, coming in 43rd position. At long last, future readiness subfactor rankings can be concluded as decent with rates in the higher midrange or even top one third.

IV. General Value of Informational Privacy

Informational privacy is understood "as the claim of an individual to determine what information about himself or herself should be known to others" (Westin 2003, p. 431) and as the demand to be protected from unwanted access to personal data (Rössler 2001, p. 25). [This] parameter […] indicates how important or unimportant [respondents from Germany consider this demand].[8]

The World Values Survey (cf. EVS/WVS 2021b) gives insight into Germany's perspective on several types of data collection. It appears that Germans seem willing to accept governmental video

[7] The paragraph from "Specifically […]" to "transformation […]" has been adopted literally from the first country report (cf. Kessel 2022).

[8] Wawra (2022, IV. 2.).

surveillance in public areas, yet oppose online monitoring of e-mails and other exchanges or data collection without consent. From all questioned participants, 66% confirm that governments should definitely or probably have the right to monitor people's behavior in public spaces (cf. EVS/WVS 2021c, p. 428) (Fig. 1).

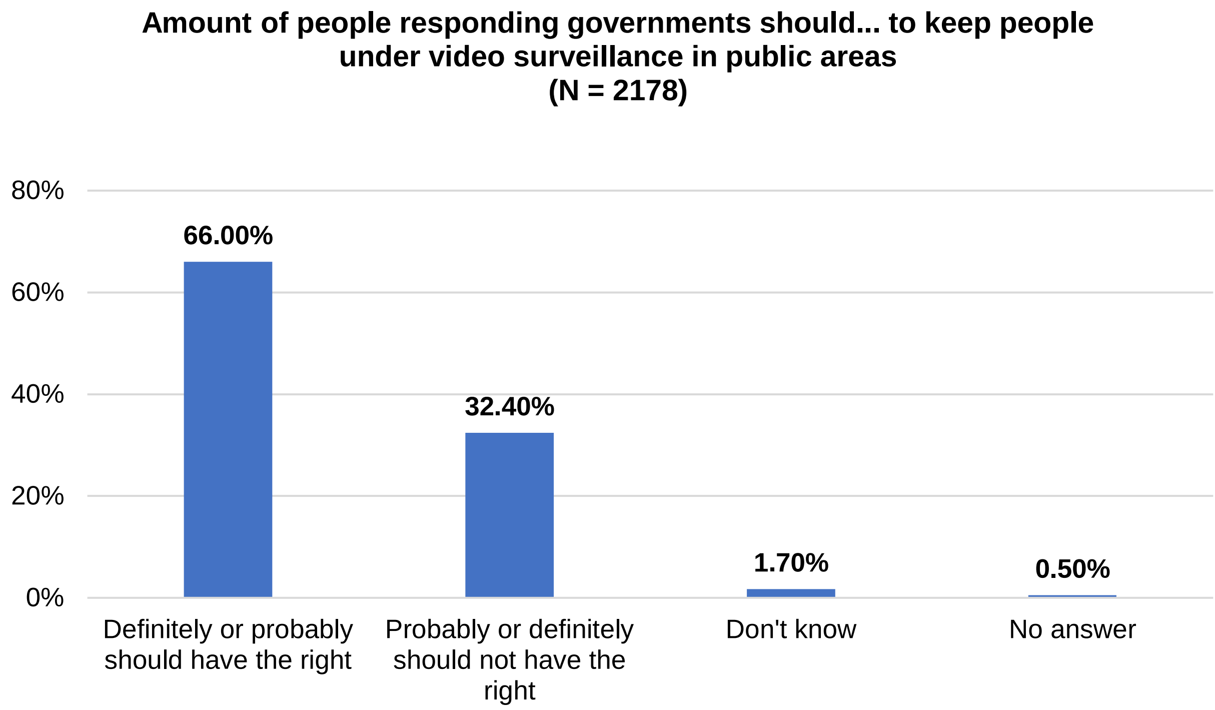

Fig. 2. Respondents' answers on governmental video surveillance (cf. EVS/WVS 2021c, pp. 428).[9]

In a contrary manner, a majority of 71.6% of Germans disapprove of e-mails and any other information exchanged online being governmentally surveilled (cf. EVS/WVS 2021c, p. 430) (Fig. 2).

[9] The collection of data was split up into separate EVS/WVS statistics; we used the data from the EVS due to bigger sample size.

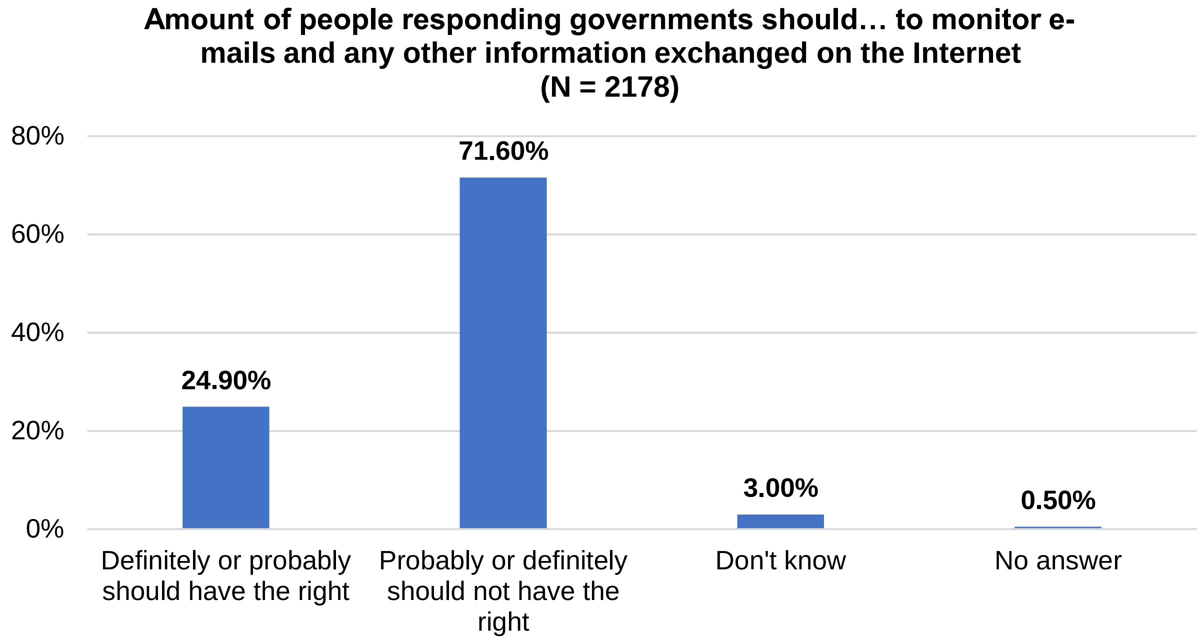

Fig. 3. Respondents' answers on governmental e-mail-monitoring (cf. EVS/WVS 2021c, pp. 432-433).[10]

Regarding another form of data collection, 81.6% of surveyed Germans opinionate that governments should probably or definitely not have the right to unknowingly collect data (cf. EVS/WVS 2021c, p. 432) (Fig. 3).

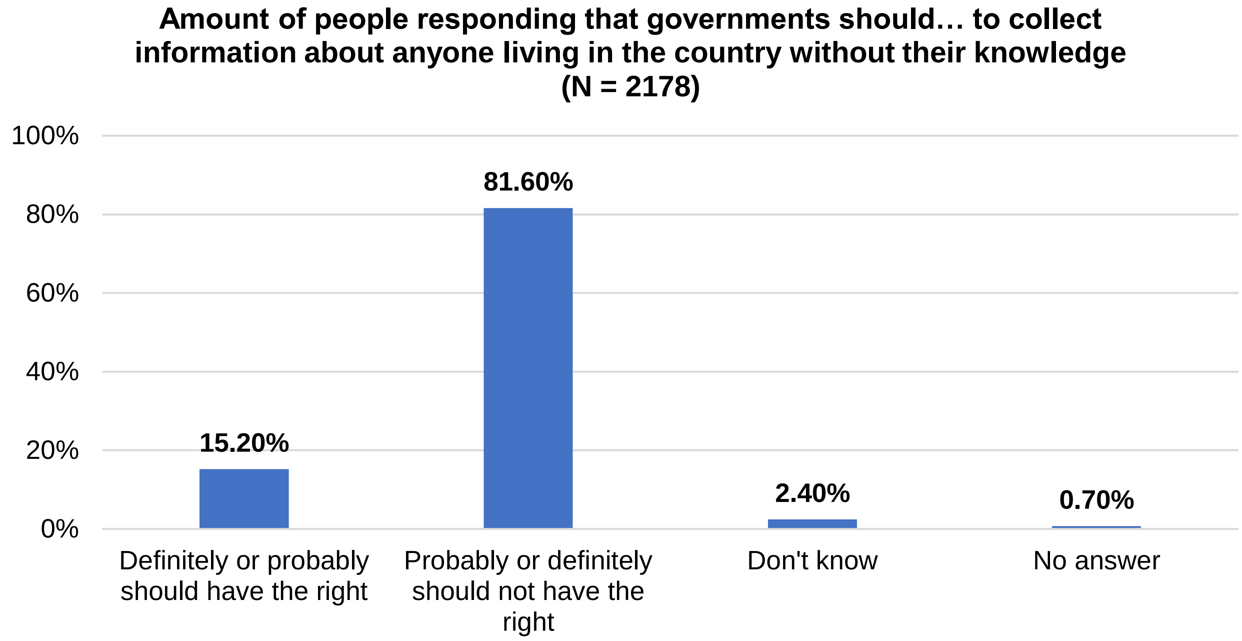

Fig. 4. Respondents' answer on governmental surveillance in terms of data tracking without consent (cf. EVS/WVS 2021b, p. 430).[11]

[10] The collection of data was split up into separate EVS/WVS statistics; we used the data from the EVS due to bigger sample size.

[11] The collection of data was split up into separate EVS/WVS statistics; we used the data from the EVS due to bigger sample size.

A majority of 56% of all German respondents agree more or less strongly with the statement that consumers should be able to refuse the corporate collection of personal data. 42% of Germans support either being paid or rewarded for disclosing their personal data. No more than 21% of respondents state not to be bothered by the corporate collection of personal information (cf. Ipsos 2019, p. 12) (Fig. 4).

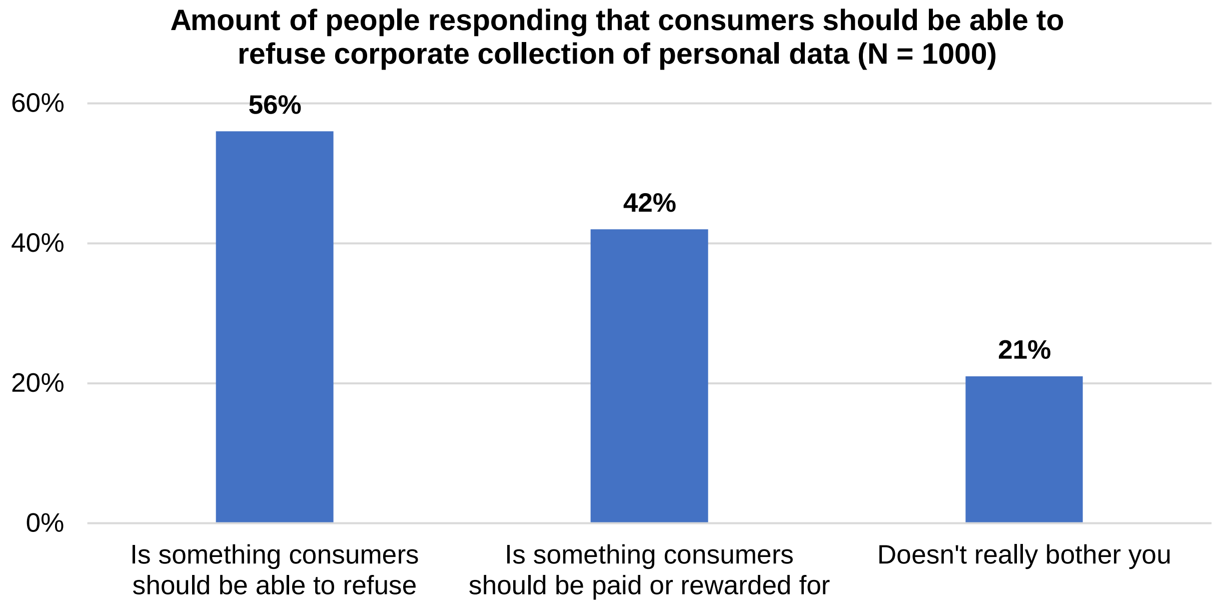

Fig. 5. Attitudes towards allowing companies to collect personal data (cf. Ipsos 2019, p. 12).

V. Degree of Privacy of Data

[This] parameter […] surveys how private or sensitive […] certain kinds of personal data [are for German respondents].[12]

In order to scrutinize sensitive types of personal information, we must firstly define the term personal data within the specific legal framework. In Germany, any type of information that refers to "[…] an identified or identifiable natural person (article 4)" is regarded as personal data (DLA Piper 2021). A natural person is considered "identifiable" by their personal data as soon as "[…] all means reasonably likely to be used […]" have been adopted (DLA Piper 2021). The identification of a natural person can be determined by several factors, some of which are a person's identification or phone number as well as their data location. Examples for identifiers online are the IP address, cookies and RFID Tags (cf. DLA Piper 2021). Additionally, there are two mechanisms along which personal data can be processed: either through a processor or a controller. In this instance, the controller is one person or a group of people deciding upon the use of the data, while the processor actually acts on the controller's behalf. Examples for processing include operation such as "[…] storage, hosting, consultation or deletion of data" about the data subject (DLA Piper 2021). In Germany, the GDPR enforces regulations upon the controller and the processer, yet it emphasizes the obligations that the processor must meet. The GDPR does not speak of sensitive personal data but of "special categories" of personal data (DLA Piper 2021). This category includes "data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics and personal data

[12] Wawra (2022, IV. 2.).

relating to criminal convictions and offences" (DLA Piper 2021). For the purpose of ensuring the privacy of these data, there are more measures and regulations that must be taken into account under German law (cf. DLA Piper 2021).

Among other things, Trepte and Masur (2016) analyzed participants' opinions regarding different types of information and their respective likeliness to impact personal privacy. Respondents had to assess several scenarios such as sharing their relationship status, political orientation, sexual orientation, as well as opting for an open profile setting and furthermore conclude how much the latter affected their privacy. Answers were located on a scale from 1 (does not affect my privacy at all) to 5 (affects my privacy very much) (cf. Trepte & Masur 2016, pp. 61-62). In terms of mean values, Germans seem to worry least about sharing their political orientation (M = 3.7), and are somewhat more concerned about disclosing their relationship status (M = 4.01) and their sexual orientation (M = 4.02). Moreover, they are most hesitant about opting for an open profile online (M = 4.55) which evidently impacts their feeling of privacy (cf. Trepte & Masur 2016, p. 62). All values lie above half the mean, indicating that these behaviors are perceived as relatively sensitive. In order to analyze the specific sensitivity of selected information, e.g. records of treatment or the amount of a person's savings, Trepte and Masur (2016) adapted a scale by Jourad and Lasakow (1958) ranging from 1 (not at all sensitive) to 7 (very sensitive), which serves as a benchmark (Fig. 5).

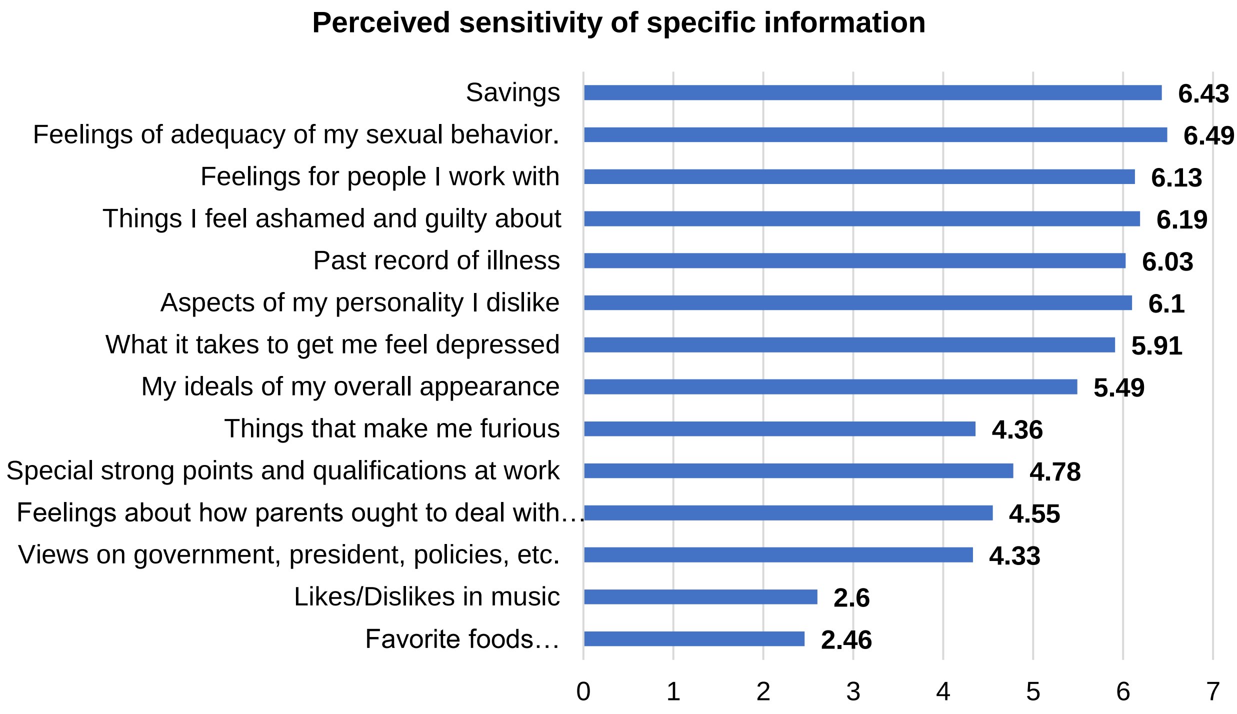

Fig. 5. Perceived sensitivity of specific types of information (cf. Trepte & Masur 2016, p. 63).

In conclusion, it appears that Germans feel most protective of information about the adequacy of their sexual behavior (6.49), closely followed by their savings (6.43), and things that lead to feelings of guilt or shame (6.19). The least sensitive categories of information are a person's favorite foods (2.46) as well as a personal taste in music (2.6).

A study published in the Harvard Business Review in 2015 gives an outlook on the extent to which different cultures including the German value different types of sensitive information. In order to compare the perceived sensitivity of certain data, prices (in US$) were assigned to said data types. The prices indicate the amount of money respondents would be willing to pay for the purpose of safeguarding their privacy (cf. Morey et al. 2015, p. 5). Analyzing answers by German respondents, one`s health history appears to be valued the most at $184.20. Government identification is another sensitive matter, the adhered price lies at over $100 and is shortly followed by credit card information that is valued at approximately $100. Additionally, data on digital communication is mentionable too, as it is assigned an estimated price of less than $50 that respondents would be willing to pay. All other analyzed types of information are given a price of about $10, while information about a person's energy use comes across as being irrelevant as mirrored by a price of $0 (cf. Morey et al. 2015, p. 5).

VI. Benefits Associated with Data Disclosure

[This] parameter […] renders the positive effects [German respondents] expect from the disclosure of their personal data.[13]

Disclosing data to companies can be beneficial in terms of saving time or money, identifying services, products and information that are of relevance to the consumer as well as being offered suitable services, products and information (cf. Ipsos 2019, p. 12). It appears that a minority of German respondents think they benefit from being provided with suitable products, services and information (29%), discovering relevant products etc. (28%), saving time (27%) or money (26%), when sharing personal data with companies. Only minimal differences between these four potential advantages in this instance (Fig. 6).

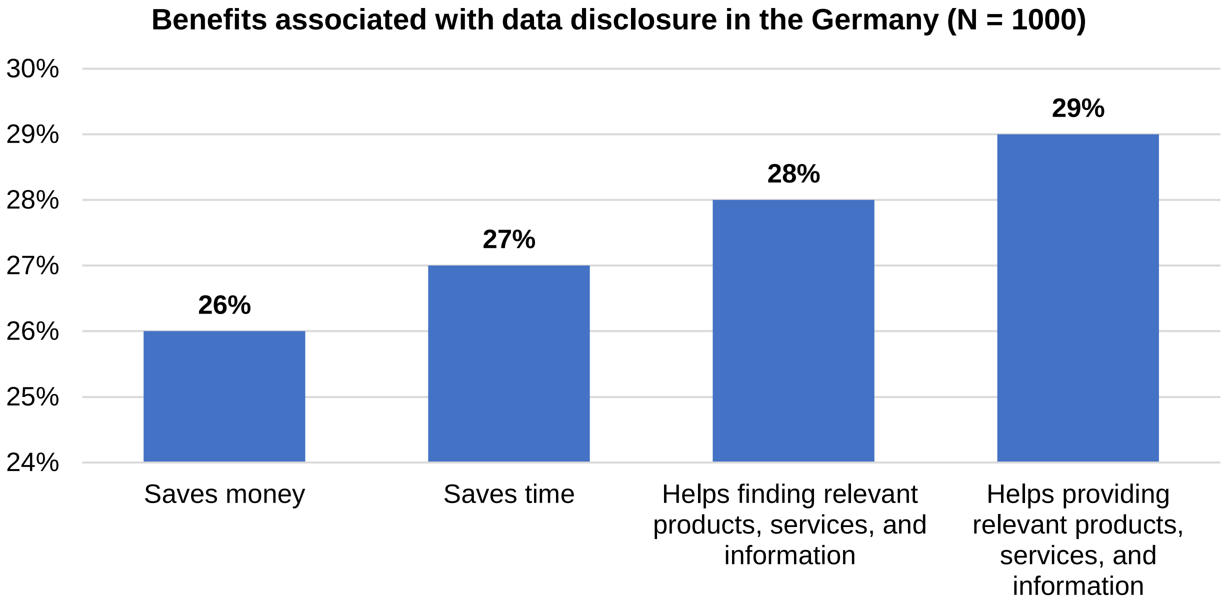

Fig. 6. Benefits associated with data disclosure in Germany (cf. Ipsos 2019, p. 12).

44% of Germans that were interrogated stated to feel more comfortable disclosing data to firms if they are rewarded with some sort of compensation, e.g. a discount in exchange for their personal information (cf. Ipsos 2019, p. 14).

[13] Wawra (2022, IV. 2.).

VII. Privacy Concerns and Risks

[This] parameter […] comprises the negative effects [German respondents] associate with data disclosure. These include their general concerns about the security of their personal data, and their control over them.[14]

1. Concerns and Risks related to Data Security

One of several data related concerns are data breaches. Germans are reluctant towards sharing personal information with companies that seem to be perceived with an apparently bad reputation in terms of data security. 59% of surveyed Germans state to feel much more or somewhat more comfortable with disclosing personal information to firms that have never been subject to any breach, leak or fraudulent usage of data and therefore have confidentiality as a top priority (cf. Ipsos 2019, pp. 13-14).

The aforementioned statement is confirmed by the fact that a majority of Germans (70%) would like to see their online data and personal information stored on a secure server. What's more, 71% of respondents indicate they would rather have their data safely secured within their country's border than abroad (33%). No more than 37% of respondents are indifferent towards their data's precise location, while 40% are not bothered by the cross-border flow of personal data collected by firms, and 35% are unbothered by governmental data leaving the country (Fig. 7). In summary, it appears that most Germans feel uneasy about their data and personal information leaving the country and being saved elsewhere.

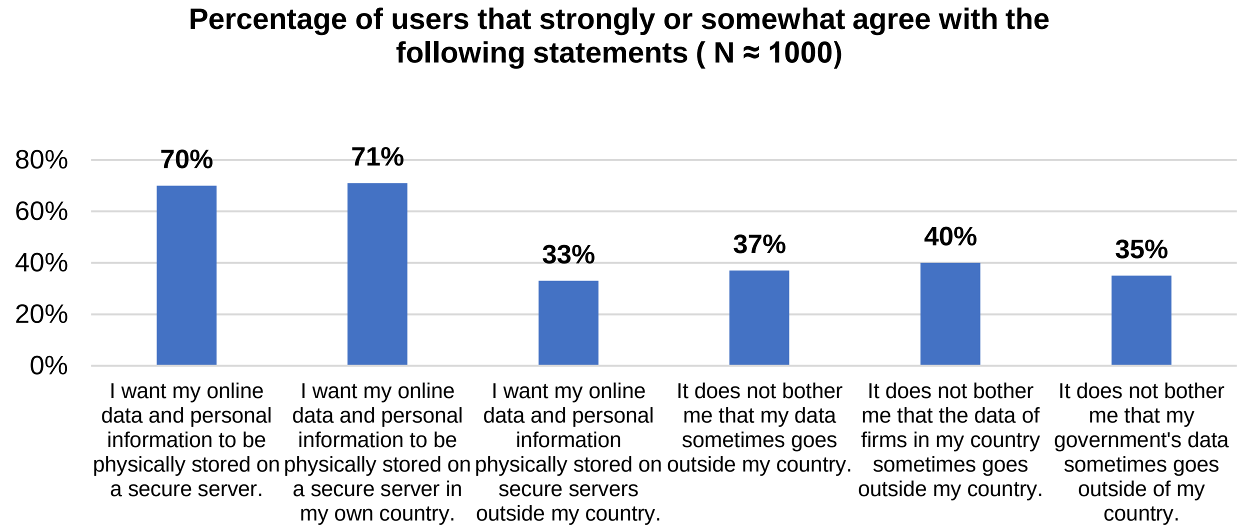

Fig. 7. Percentage of users that strongly or somewhat agree with the respective statements (cf. CIGI-Ipsos 2019b, pp. 13-23, 2019c, p. 283).

2. Concerns and Risks related to Data Control

Trepte and Masur (2016) state that Germans are extremely aware of the risks involved with an open Social Media profile e.g. data abuse as well as those of uploading pictures. On a 5-point Likert Scale ranging from not at all likely (1) to very likely (5) that indicates the perceived risk, Germans feel that opting for an open profile (M = 4.27) or posting pictures (M = 3.92) are both very risky, yet the open profile is considered more of a peril (cf. Trepte & Masur 2016, pp. 40-41)

[14] Wawra (2022, IV. 2.).

The perceived amount of control over one's own data correlates with the participant's age. Rated on a 4-point Likert scale ranging from 1 (I totally agree) to 4 (I totally disagree), it appears that younger respondents (M = 1.81) seem to have more control over their privacy settings for data shared on Social Networking Sites (SNS) than older participants (M = 2.21) (cf. Kowalewski et al. 2015, p. 819). This finding may be explained by the fact that younger generations have grown up with modern technologies and consequently are more familiar with privacy related practices.

In their jointly conducted study, the *Center for International Governance Innovation* and *Ipsos Public Affairs* (CIGI-Ipsos) focus on dismantling changes in data related behavior based upon generally underlying privacy concerns (cf. CIGI-Ipsos 2019). When being asked about trust issues that affect daily Internet use, 28% of surveyed Germans claim to disclose less personal information online due to lack of trust, while 24% report to use the Internet more selectively. Distrust of the Internet has led to 23% of respondents seeing to securing their personal devices regularly, 15% self-censor the content they share online or what they say online, yet no more than 9% have limited their online purchases (Fig. 8).

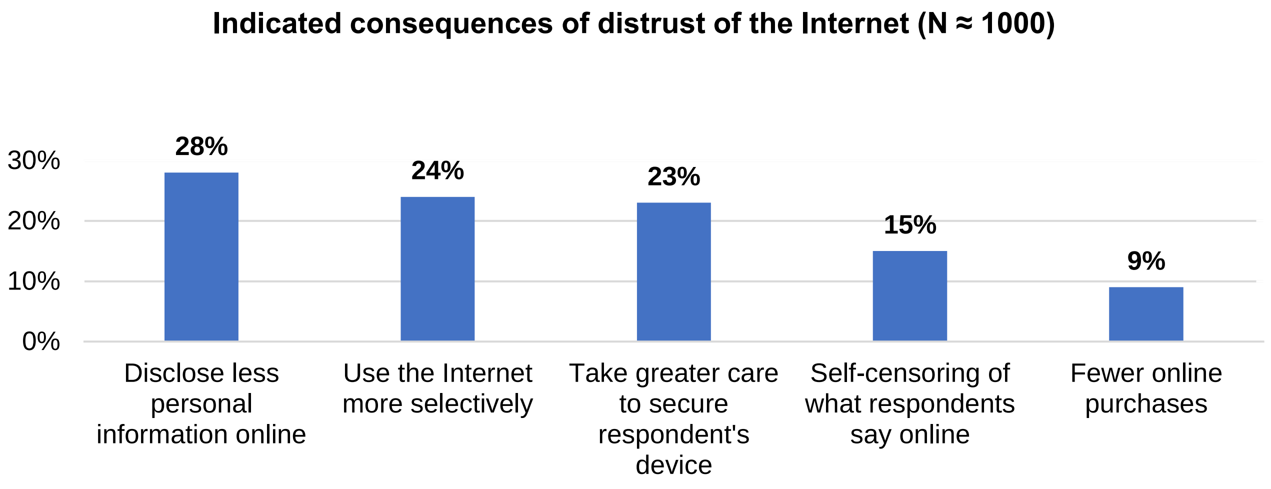

Fig. 8. Consequences of distrust of the Internet (cf. CIGI-Ipsos 2019c, p. 24).

VIII. Data Protection Literacy

[Data Protection Literacy] captures [Germans'] awareness and knowledge of data protection, privacy rules and policies as well as the skills they report to have, and the measures they take to protect their personal data.[15]

A majority of Germans (59%) claim to be very or somewhat aware of currently applicable data protection and privacy rules in their home country. This places the country in second rank in terms of their comparably very high data protection knowledge, directly after India. Nevertheless, 42% of surveyed Germans state not to be very aware if not aware at all of current data protection and privacy rules (cf. CIGI-Ipsos 2019c, p. 281) (Fig. 9).

[15] Wawra (2022, IV. 2.).

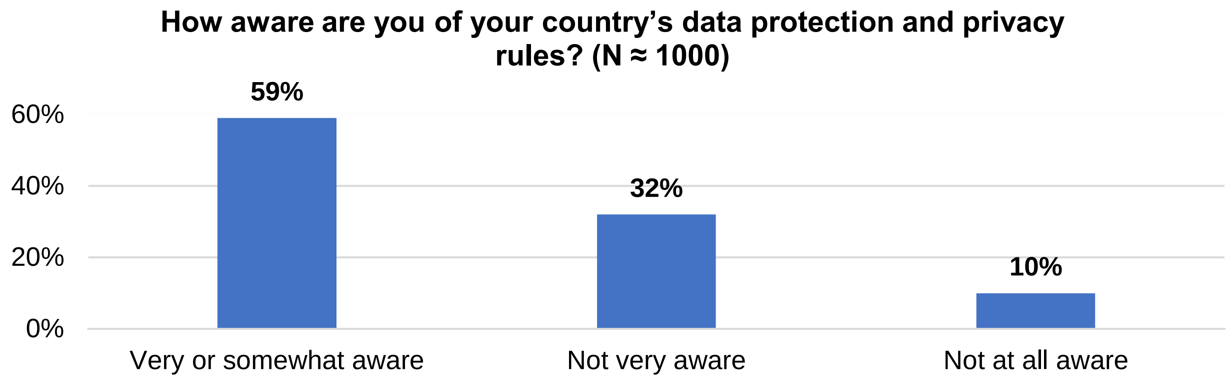

Fig. 9. Awareness of data protection and privacy rules in Germany (cf. CIGI-Ipsos 2019c, p. 281).

Germans' overall knowledge about data protection as well as measures to strengthen a private user's cyber security appears to be no more than mediocre. Therefore, Germans cannot be viewed as fully up to date as indicated by general knowledge scores of IT security terms. Based on a 5-point rating scale by Rohrmann, ranging from 1 (I disagree) to 5 (I strongly agree), more than half (54%) of all Germans respondents admit to not being well informed about data exploitation. Only 35% of participants state to strongly or fairly agree with the fact that the choice of a certain operating system has an influence on a person's data security. While approximately one third (35%) of all surveyed Germans indicate to moderately agree with the former statement. Only one quarter of Germans do not seem to be familiar with the phenomenon of "online phishing", as stated by 25% of surveyed people. Additionally, a majority of 60% of respondents claim to strongly (34%) or fairly agree (26%) to be aware of mechanisms that encrypt e-mails (cf. Herbert et al. 2020, pp. 6-7).

A condensed version of the Online Privacy Literacy Scale (OPLIS), designed by Trepte and Masur (2017), gives insight into the objectively measured declarative and procedural knowledge about online privacy in Germany. Among other subjects, declarative knowledge is measured by questioning participants about their understanding of data collection or usage behavior by service providers and institutions, or data protection laws and directives. Furthermore, procedural knowledge questions cover data protection strategies (cf. Trepte & Masur 2017, p. 43). Results from the survey indicate a lack of knowledge about online privacy and related topics within the German population. Apparently, a large number of participants seem to be rather uninformed and could only answer half of the questions. Concerning knowledge about institutional practices of data collection within the dimension of declarative knowledge, 24% of respondents appear to be indifferent towards data collection practices undertaken by the National Security Agency. Additionally, more than half of all participants (55%), appear to be unaware of the fact that every user of online applications has the right to inquire the precise information that is being saved by the application (cf. Trepte and Masur 2017, p. 43).

Results from a study conducted by Herbert et al. show that close to half (47%) of German participants come across as being moderately informed about data security. Another 31% of respondents are assigned to the category of low security knowledge, while the smallest amount of people (22%) gives the impression of being well informed (cf. Herbert et al. 2020, p. 8).

Analyzing Germans' security behavior, based on yes-no-questions, however, a majority of 82% of respondents specify to use anti-virus software. Another popular security measure is the use of a protected e-mail provider, as claimed by 76% of surveyed Germans. 51% of respondents state to use the end-to-end encryption of their e-mail. The least attractive security measure among Germans appears to be the use of a VPN-client, which secures anonymity online (20%) (cf. Herbert et al. 2020, p. 7).

Percentage frequencies for security behavior, measured with a 5-point rating scale, stipulate that 61% of respondents fairly (20%) or strongly agree (41%) with installing recent updates for their operating systems as soon as possible. A 54% majority of surveyed Germans claim to completely vary within their choice of password for each used online service. Yet, no more than 37% of respondents fairly (22%) or strongly agree (15%) to adapting default settings of applications in order to profit from increased data security. Only 23% of Germans profess that they use separate browsers for online banking and other services, while even less participants (13%) use a different e-mail address for each online service (cf. Herbert et al. 2020, pp. 7-8).

Visual anonymity on social networking sites is another privacy strategy in the country, yet rather unpopular. 35.6% of Germans opt for an avatar or logo as a profile picture. Another 27.1% of participants claim to use a photo of themselves in which they are not fully recognizable. Only 6.8% of respondents seem to not have any kind of visual profile image (cf. Trepte & Masur 2016, p. 56). Even less adapted strategies include the pseudonymization of names, or restrictive visibility of online tweets (cf. Trepte and Masur 2016, pp. 56-57).

In line with Germans' self-assessed high knowledge of institutional data protection and privacy rules, 64% of all respondents assert to protect their data and seem confident in their doing so. Nevertheless, this majority is subdivided into only 11% of Germans that strongly agree to sufficiently protect their personal data while a sub-majority of 53% somewhat agrees with the former (cf. CIGI-Ipsos 2019b, p. 29, 2019c, p. 283).

The category of low security knowledge contains one third of Germans (33%), and only 24% of all respondents appear to go the full length in order to secure their privacy online (cf. Herbert et al. 2020, p. 8). As indicated by 53% of respondents only somewhat agreeing to protecting their private information at all costs (cf. CIGI-Ipsos 2019b, p. 29, 2019c, p. 283), it seems unsurprising, that 43% of Germans actually implement no more than moderate security skills in their behavior.

Demographics evidently have a significant influence on data protection literacy. Men and women indicate different levels of privacy knowledge, age appears to play an important role, so does the educational background and political orientation of questioned participants. Comparing security and privacy know-how of women and men on a 5-point Likert scale from 1 (I disagree) to 5 (I agree) indicating familiarity with security measures or risks, men (M = 3.05) are slightly more informed than women (M = 2.64). Yet, the overall knowledge is moderate for all sexes (cf. Herbert et al. 2020, p. 9). Trepte and Masur report similar findings. Their study shows that women are able to answer an average of 4.57 out of 10 privacy related questions correctly, while men are slightly more cognizant and able to answer an average of 5.39 questions correctly. The average of all German participants lies at 4.95 from 10 questions being answered correctly, and therefore indicates a merely moderate knowledge level in Germany (cf. Trepte & Masur 2017, p. 44). The gender gap within security knowledge of men and women can therefore be seen as a significant aspect of online data protection literacy (cf. Herbert et al. 2020, p. 10).

Additionally, age is an essential attribute influencing online data protection literacy. When clustering participants from the Trepte and Masur study from 2017 into five age groups, the 25- to 39-year-olds stand out as being the most knowledgeable. The aforementioned group can be considered most cognizant, as participants answered 6.11 from 10 data related questions correctly, and their understanding was substantially above the overall average (4.95). Participants aged 24 and younger (5.83) and those between age 40 and 54 (5.69), appear to be rather literate regarding subjects linked to online privacy and data protection. Moreover, the two age groups that include participants older than 55 seem to be less informed. Their number of correct responses (4.92 and 3.60) lies below the German average of 4.95. Nonetheless, participants in the oldest age group (aged 70 +) are without doubt the least literate (3.60) (cf. Trepte & Masur 2017, p. 44).

A study conducted in 2015 by Sylvia Kowalewski et al., furthermore scrutinizes the levels of perceived usability, control and knowledge of privacy settings in Social Networking Sites (SNS) among participants from different age groups using a 4-point Likert scale ranging from 1 (I totally agree) to 4 (I totally disagree). In this setting, respondents are assigned one of two groups. The younger group includes participants aged 20-30, while the older group's participants are aged 31-66 years. Comparing mean values, the younger group indicates a higher feeling of control over their data (M = 1.81) while the older group indicates to feel less in control (M = 2.21). What's more, younger SNS users are comparably a lot more informed about privacy settings that can ensure data protection than the older users. Opposingly, it becomes clear that older network users (M = 2.46) assess the usability of SNS's privacy settings to be slightly more intuitive than participants in the younger age group (M = 2.72) (cf. Kowalewski et al. 2015, p. 819).

Participants with a university entrance certificate exceed the average of literacy in Germany, and hence are very aware of data protection. This indicates that there is a direct link between the educational background of an individual and online privacy literacy (cf. Trepte & Masur 2017, p. 44). Based on a 5-point rating scale from 1 (I disagree) to 5 (I strongly agree) , it is proven to be statistically significant, that German respondents with high education (M = 3.12) are stated to be quite knowledgeable of online measures that secure personal information, while those with a medium (M = 2.85) and low level (M = 2.67) of education seem to be less aware (cf. Herbert et al. 2020, p. 9).

Finally, it becomes clear that political orientation has a certain effect on security knowledge scores in Germany. Herbert et al. (2020) chose a scale for political orientation sectioned into left-wing, fairly left-wing, in the middle, fairly right-wing and right-wing, mirroring a simplified version of the political spectrum from left to right. The authors do not mention any particular parties in this instance. Security knowledge was measured on a 5-point scale ranging from 1 (I disagree) to 5 (I strongly agree) indicating familiarity with certain topics and knowledge is highest among participants that claim to support fairly right-wing politics (M = 3.05). Respondents that are politically fairly left-wing orientated, appear to be similarly aware (M = 3.02). Left-wing oriented (M = 2.91) Germans or those who position their political beliefs in the middle (M = 2.82) seem to be less literate. Interestingly, however, the lowest level on the digital knowledge and security score is assigned to Germans that state to be right-wing oriented. Overall, participants that consider themselves to be either fairly left- or fairly right-wing are most knowledgeable (cf. Herbert et al. 2020, p. 9).

An analysis by Schenk et al. (2012) categorizes Germans into three groups in relation to their data disclosure behavior (cf. Schenk et al. 2012, p. 46). 48% of participants are included in a group that discloses very little personal information. The group is characterized by people that deeply care about their privacy, and therefore try to minimize their online interactions. When communicating online, they prefer exchanges with friends, yet avoid interaction with unknown SNS users at all cost. 20% of participants furthermore state to pseudonymize their real name. Overall, participants in this cluster use privacy settings restrictively. This points at the fact that the aforementioned respondents are very aware of data policies and know how to adapt given measures. Respondents included in this cluster tend to be older, have received a formal education, cannot be viewed as early-adopters, and do not use networks such as Facebook regularly (cf. Schenk et al. 2012, pp. 47-48). People that can be considered privacy managers shape the second group that makes out 39% of all participants. Privacy-managers are comparable to people that disclose little information, as they actively apply privacy settings. Nevertheless, they expose a significant amount of data about themselves online but preferably share posts and information with a small circle of close friends. This group does not have a problem with communicating via online tools, as they are very knowledgeable about privacy settings and can efficiently alternate and manage privacy settings. Participants included in this group are middle aged and have received a formal education (cf. Schenk et al. 2012, pp. 47-48). A minority of 14% of participants seem to share a lot of personal information online. Here, the main goal of online communication is making new acquaintances. In order to maximize possible interaction with others, privacy settings are only applied in a lax manner. This cluster includes mainly young people with a lower educational level (cf. Schenk et al. 2012, pp. 46).

In conclusion, these findings insinuate that most Germans claim to be aware of data protection policies and regulations in their country. Yet, the analysis of overall knowledge levels of IT terms and privacy strategies demonstrates a discrepancy between beliefs and effective data protection management. The actual level of online literacy in Germany can be described as moderate. In contrast, however, most respondents seem to evaluate their own privacy skills highly, and believe to take more than enough measures to protect their personal information online. A few privacy supporting strategies such as the use of anti-virus software, a protected e-mail provider, or end-to-end encryption seem to be appealing to quite a lot of Germans, while the use of a VPN-client seems to be adapted by less.

In addition, it becomes clear that data protection literacy differs between demographic groups. Gender, age, education and political orientation all have an impact on a person's privacy literacy. Overall, men are more literate than women, and younger generations seem more likely to take privacy related measures. However, very young, less educated Internet users are considered to disclose a vast amount of information online without adapting any privacy settings, while highly educated middle-aged people have the tendency to manage privacy settings closely and restrictively. Moreover, a high level of education leads to an improved data protection literacy in society and people that consider themselves politically fairly right-wing oriented appear to be the most aware of privacy protection and related settings.

IX. Attitudes Towards Data Receiver

[This] parameter […] refers to [Germans'] attitudes towards institutions to which they disclose their data. These comprise above all their trust in national and foreign governments and (different kinds of) companies pertaining to the protection and correct use of their data.[16]

A majority of Germans appear to not trust other people easily, as indicated by more than half of the respondents (55.90%) who answered that you can't be too careful with other people (cf. EVS/WVS 2021a, p. 7) (Fig. 10).

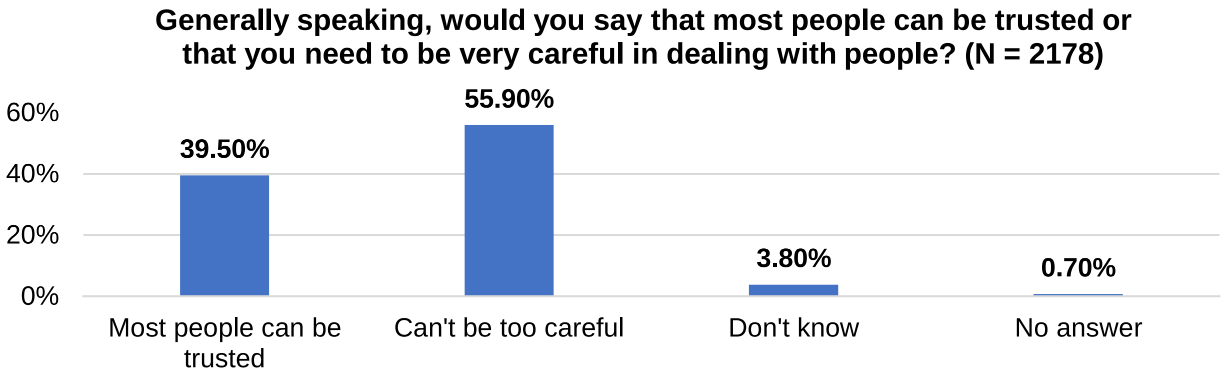

Fig. 10. General trust towards people in German society (cf. EVS/WVS 2021c, p. 172).[17]

Evaluating the numbers shown above, most Germans seem to be rather distrusting. Consequentially, this finding might be one of many reasons for the prevailing data disclosure behavior within the country. In the subsequent passages, German attitudes towards two large groups of data receivers are analyzed: the government and companies. These can influence their data disclosure behavior.

1. Attitudes Towards Governments

Overall, Germans indicate low trust levels towards their institutions' data protection regulations. As shown in the World Value Survey (cf. EVS/WVS 2021c, pp. 264, 271, 273), a majority of Germans spoke up about feelings of distrust towards their government, political parties as well as parliaments. Yet, the lack of confidence in individual political parties stands out the most (77.3%) (Fig. 11).

[16] Wawra (2022, IV. 2.).

[17] The collection of data was split up into separate EVS/WVS statistics; we used the data from the EVS due to bigger sample size.

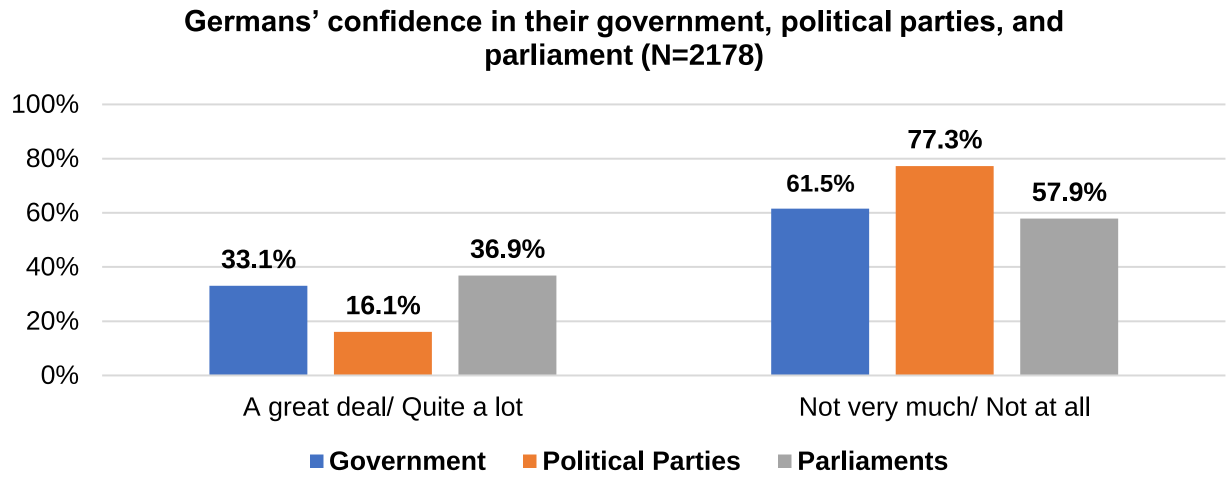

Fig. 11. Germans' confidence in their government, political parties, and parliament (cf. EVS/WVS 2021c, 264, 271, 273).

Based on results from the Ipsos survey in 2019, Germans generally do not trust governments with the use of personal data. Hence, no more than 37% of respondents trust their national government to use personal data rightfully. In terms of foreign governments, trust levels are even lower, as indicated by a meagre 12% of respondents (Fig. 12).

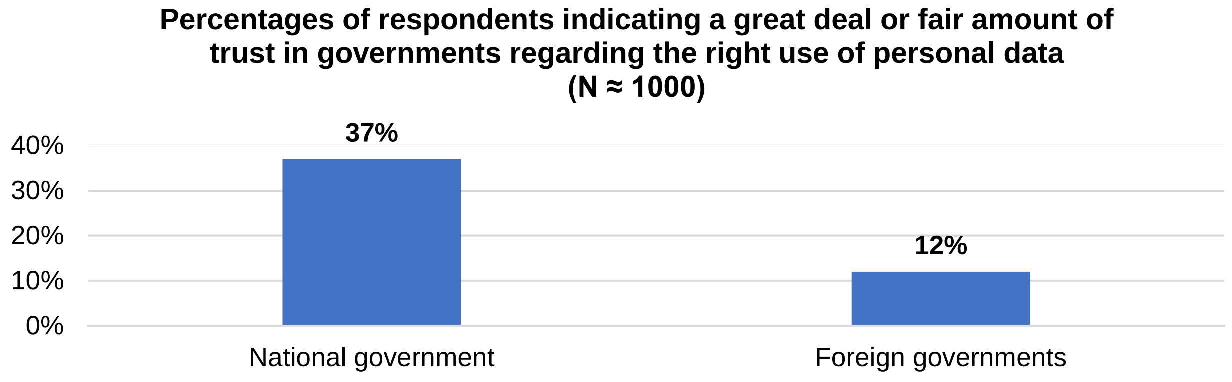

Fig. 12. Percentages of respondents indicating a great deal or fair amount of trust in governments regarding the rightful use of personal data (cf. Ipsos 2019, p. 20).

Taking it further, national and foreign governments appear to have a negative impact on Germans' overall trust in the Internet. A majority of 64% of respondents express that national governments contribute to their distrust of the Internet. Even more Germans (68%) claim that distrust is enhanced by foreign governments (cf. CIGI-Ipsos 2019a, p. 117, 2019c, p. 20). A reason to why governments have this exact impact was not elaborated. Adding further causes of distrust of the Internet, 21% of surveyed Germans indicate that their behavior was affected by their national governments' control over the Internet. In line with Germans' high distrust level towards foreign institutions, 29% of Germans believe that foreign governments' control over the Internet shapes their distrust (cf. CIGI-Ipsos 2019a, p. 22) (Fig. 13).

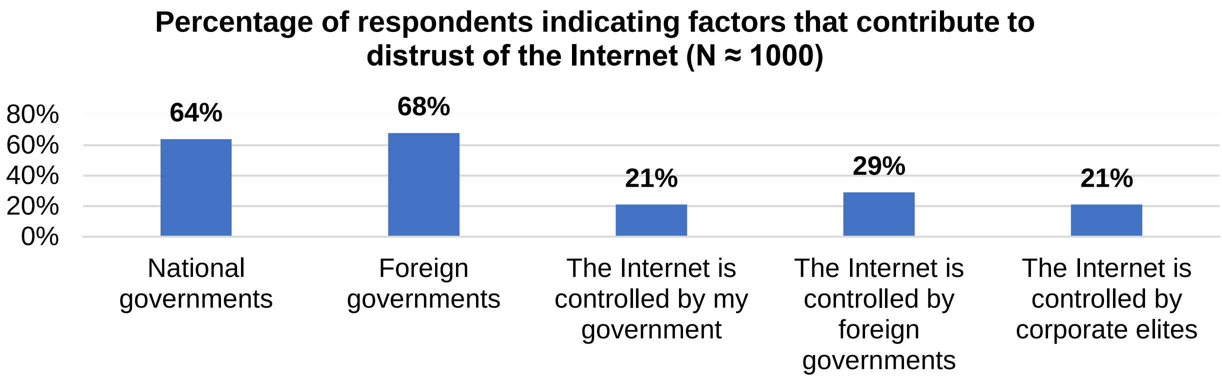

Fig. 13. Percentages of respondents indicating factors that contribute to distrust of the Internet (cf. CIGI-Ipsos 2019a, p. 117, p. 119, 2019c, p. 20, p. 22).

2. Attitudes Towards Companies

Comparable to the trust in governments, confidence in major companies appears to be very low in Germany. When being asked about whether large firms appear trustworthy, only 20.5% of respondents state to trust them a great deal or quite a lot. The majority (71.6%) of surveyed Germans assume major firms not to be very trustworthy, if not untrustworthy (cf. EVS/WVS 2021c, p. 275)[18].

Comparing governmental with corporate data protection, Germans tend to trust companies more referring to their abilities to secure data. More than half (51%) of the respondents agree with the statement that companies sufficiently protect personal information. As indicated by 41% of Germans, there appears to be less confidence in governmental security of private information (cf. CIGI-Ipsos 2019b, p. 45, p. 47, 2019c, p. 283) (Fig. 14).

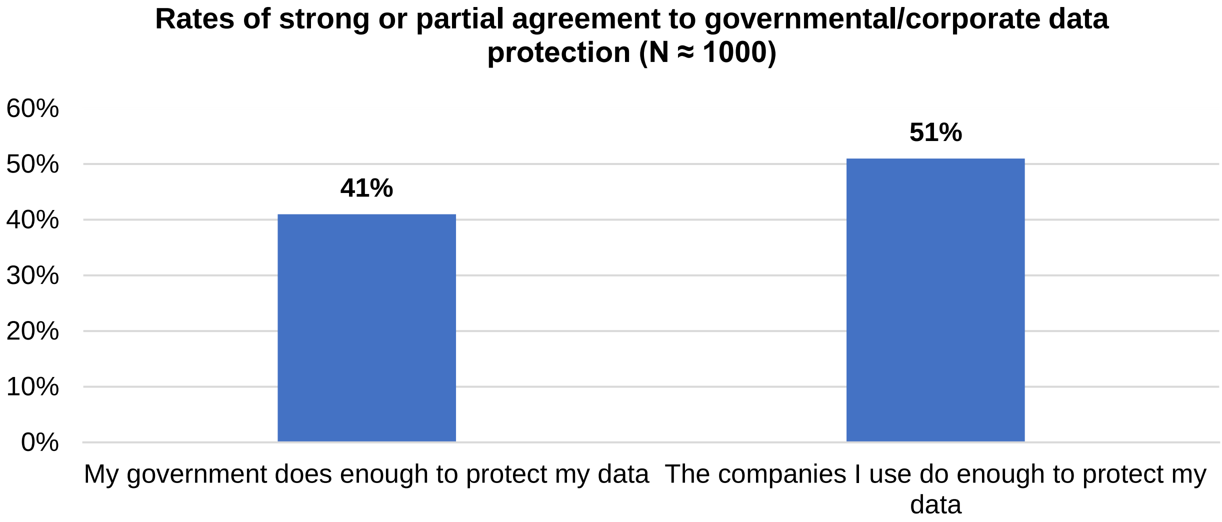

Fig. 14. Percentage of respondents that strongly or somewhat agree to governmental and corporate efforts for data protection (cf. CIGI-Ipsos 2019b, p. 45, p. 47, 2019c, p. 283).

[18] The collection of data was split up into separate EVS/WVS statistics; we used the data from the EVS due to bigger sample size.

Figure 15 points out to which extent Germans trust selected types of companies. It manifests, that healthcare providers, financial service companies, and shipping/ delivery companies are seemingly the most trustworthy, with healthcare providers being at the top of the list. Furthermore, there does not only seem to be a discrepancy between confidence levels regarding data protection between governments (national and foreign) and companies, but also depending on which industry a company operates in.

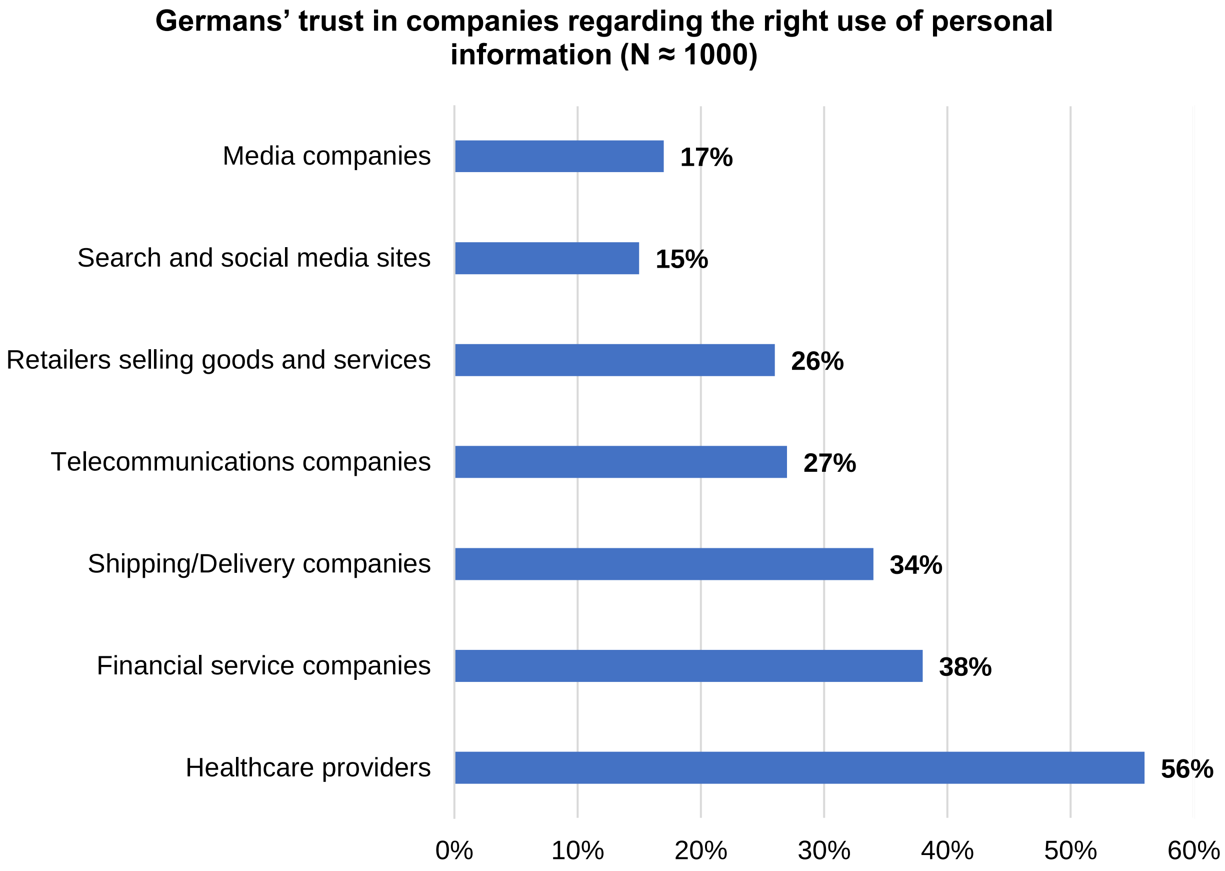

Fig. 15. Germans' trust in companies regarding the right use of personal information (cf. Ipsos 2019, p. 20).

Telecommunication companies (27%), retailers selling goods and services (26%), search and Social Media sites (15%), and media companies (17%) are placed at the bottom end of the spectrum and seem suspect. Nonetheless, search and social media sites are valued to be the least reliable in adhering terms of data disclosure. What stands out is that a majority of respondents state to trust healthcare providers, all other industries are perceived as trustworthy within their right use of data by a minority of German respondents. (cf. Ipsos 2019, p. 20) (Fig. 15).

Moreover, 68% of Germans that were surveyed, state that companies in general have contributed to intensified data privacy concerns throughout the last year. When comparing different types of companies, 80% of respondents specified Internet companies in particular had the aforementioned effect on confidence levels over the same period of time (cf. CIGI-Ipsos 2019c, p. 7). In addition, a 74% majority of Germans report that Social Media companies are one of many reasons to distrust the Internet (cf. CIGI-Ipsos 2019c, p. 20). Additional contributors to distrust of the Internet are Social Media companies, search engines, Internet providers, e-commerce platforms as well as online and mobile banking platforms. As indicated by 74% of respondents, Germans appear to have the lowest level of trust towards Social Media companies. Moreover, 64% of Germans view search engines as another factor that enhances their general distrust of the Internet. Internet Service Providers (55%) and E-commerce platforms (57%), mark the middle field on the distrust scale, whilst Online and mobile banking platforms seemingly have little effect on distrust levels (44%) (Fig. 16).

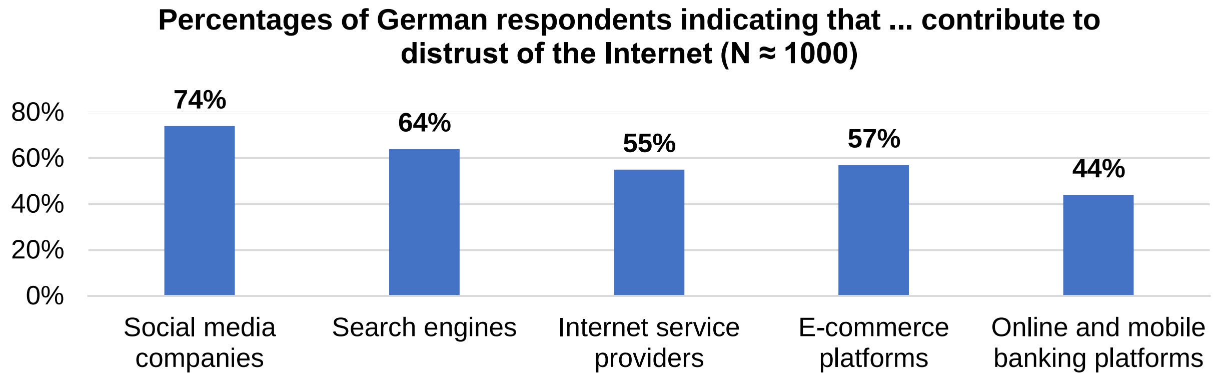

Fig. 16. Percentages of German respondents indicating that the mentioned media, platforms, or industries contribute to distrust in the Internet (cf. CIGI-Ipsos 2019c, p. 20).

X. Communication on Data Use

[This] parameter […] relates to the importance [German respondents] attribute to communication on how their personal data are used.[19]

Companies or brands that offer transparent data processing tend to gain consumers' trust more easily. A majority of more than 60% of respondents claim to be much or somewhat more comfortable with sharing personal information with a corporation, if users are clearly informed about how their data will be protected and where it is stored. Another measure that eases Germans' data disclosure related distrust in brands and companies is the promise of a firm not to share or sell data to third parties, as indicated by 55% of respondents (cf. Ipsos 2019, p. 14) (Fig. 17). In addition, 38% of respondents clarify that they would be less reluctant to disclose personal information to firms or governments if they are fully informed about all risks the user may be exposed to (cf. Ipsos 2019, p. 17).

[19] Wawra (2022, IV. 2.).

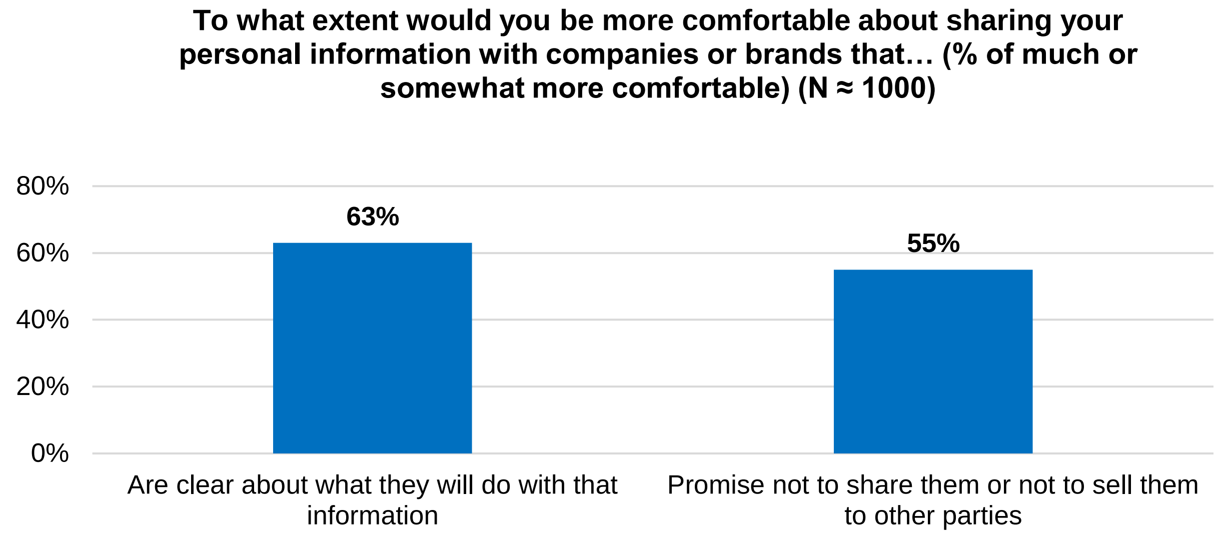

Fig. 17. Communication on data use (cf. Ipsos 2019, p. 14).

XI. Key Findings

This chapter focuses on summarizing all significant results taken away from the analysis of surveys and studies covering aspects that may have an influence on data disclosure behavior. The findings indicate which attitudes, values and views can have an impact on whether a user decides to disclose or withhold private information online. The following pages give an overview of prevailing opinions in Germany regarding informational privacy, commonly used data protection strategies and the perception of data control. The insights gained from this study should facilitate future cross-cultural comparison. Additionally, we mention interesting research gaps that became apparent during this analysis.

1. Digital Competitiveness

In terms of digital competitiveness, Germany has been ranked in 18th position in the IMD Digital Competitiveness Ranking in 2021. Ever since 2017 there has been little improvement in the country's overall performance, with 17th rank in 2017 and 2019 marking highlights. The most recent ranking outlines the country's strength in digital training and education (rank 17) with a high pupil-teacher ratio (rank 3) and a considerable number of graduates (rank 3) in the scientific field. Outstanding ranks for robots in education and R&D (rank 2) , and high expenditure rates for research and development (rank 8) point out Germanys focus on scientific concentration (rank 6). In terms of capital (rank 23), Germany is the country with the best credit ratings (rank 1). On the other side, digital shortcomings include general technical skills (rank 54) and substandard quality in terms of communications technology (rank 55) and the amount of mobile broadband subscribers (rank 56). Regarding business agility (rank 15) in Germany, the identification of opportunities and problems (rank 55) seems to be a hurdle, additionally, the use of big data and analytics (rank 53) does not seem to be widespread.

2. General Value of Informational Privacy

The findings show that most Germans (66%) appear to tolerate governmental video surveillance in public areas. However, a majority of Germans (71.6%) refuse governmental e-mail monitoring or monitoring of any type of online communication. Even more Germans (81.6%) are strictly opposed to governmental data collection without consent. In terms of corporate data collection, most participants (56%) indicate that all Internet users should be able to completely impede corporate collection. Nevertheless, the analysis has proven that many Germans (42%) feel less negative about data collection when they are rewarded for their personal information in exchange. Only few participants (21%) claim to be unbothered by corporate data collection.

3. Degree of Privacy of Data

In Germany, information that refers to an identified or identifiable natural person is considered personal data, e.g. personal identification numbers, phone numbers and data location. A person's IP address, cookies and RFID Tags can lead to a person being identifiable in an online context. Furthermore, the GDPR mentions a special category of data that includes data relating to:

- Race (stated as such in the law)
- Religion
- Sexual Life
- Health
- Genetics
- Biometrics
- Criminal convictions and offences.

Regarding the degree of privacy of data, with items placed on a 7-point scale from 1 (not at all sensitive) to 7 (very sensitive), it can be seen that German SNS (Social Networking Sites) users feel extremely protective about data that relate to their sexual behavior (6.49), personal savings (6.43), or things they feel guilty about or ashamed of (6.19). Additionally, Germans are willing to pay a substantial price for safeguarding the privacy of data covering a person's health history ($184.20), government identification (over $100) and credit card information (approximately $100).

4. Benefits Associated with Data Disclosure

When being asked for an assessment of given benefits linked to data disclosure, only minorities stated that saving money (26%) and time (27%), improving consumer search for relevant products, services and information (28%) and companies providing users with relevant products, services and information (29%) were emerging benefits. 44% of respondents regard compensation or receiving an incentive from the collecting company as another positive outcome from data disclosure.

5. Privacy Concerns and Risks

Gathered survey findings analysing privacy concerns and risks are split into two subitems: data security and data control.

a. Data Security

Confidentiality appears to be a top priority for data disclosing Internet users. Therefore, many Germans object sharing personal information with companies that have been subject to a data breach or leak. This explains why most Germans (59%) indicate to feel a lot more comfortable with disclosing information to firms that have not been associated with a data breach, leak or fraudulent behavior in the past. Regarding cross-national data flow, it becomes clear that most Germans (71%) prefer personal data to be stored on a secure server within Germany rather than on a secure server abroad (33%). Other participants state to be unbothered by data in general (37%), corporate data (40%), or governmental data (35%) leaving the country.

b. Data Control

Social Media usage and publicly shared content are associated with high risk in Germany. Rated on a scale from not at all likely (1) to very likely (5) that indicates perceived risk, Germans perceive both an open Social Media account (M = 4.27) and photos uploaded online (M = 3.92) as rather risk related. Additionally, felt levels of control vary between age groups. Due to know-how about applying privacy settings and rated on a scale from 1 (I totally agree) to 4 (I totally disagree), younger participants (M = 1.81) feel more in control of their privacy, than older participants (M = 2.21). As a result of privacy concerns, some Germans see to disclosing less data online (28%), using the Internet more selectively (24%), securing personal devices regularly (23%), self-censoring online content (15%) or limiting their online purchases (9%).

6. Data Protection Literacy

59% of Germans estimate their own knowledge as well as awareness of data protection and privacy to be rather high. Yet, IT knowledge questions about strategic measures that ensure online privacy as well as a condensed version of a scale designed to measure online privacy literacy show the opposite. In fact, 47% of Germans can be described as only moderately aware of data security and related measures. Only a small amount (22%) of surveyed Germans appear to be highly informed. More than half of the surveyed people (65%) assume they protect their personal information online sufficiently, yet a lot of Germans' (43%) security skills are as a matter of fact on a moderate level, shortly followed by those with low skills (33%) and only 24% with high skills. Popular security strategies are the use of an anti-virus software (82%) or a protected e-mail provider (76%), whereas the use of a VPN-client (20%) is quite unpopular. Regarding age groups and their online protection literacy, 25- to 39-year-olds indicate to be most cognizant with 6.11 out of 10 privacy related questions being answered correctly. Generally speaking, younger people (M= 1.81) can be considered more literate than older people (M=2.21) in terms of privacy settings and the resulting control. Both aforementioned items are rated on a 4-point Likert scale ranging from 1 (I totally agree) to 4 (I totally disagree). On a 5-Point Likert scale from 1 (I disagree) to 5 (I agree) indicating familiarity with security measures, gender effects on privacy and security know-how become apparent and indicate that men (M = 3.05) are slightly but significantly more literate than women (M = 2.64) in Germany. Moreover, people with a high level of education are more aware than the average German. Lastly it seems that people who consider their political orientation to be only fairly right-wing (M = 3.05) or fairly left-wing (M = 3.02) are most knowledgeable of security measures that safeguard online privacy, while people who consider themselves politically right-wing (M = 2.58) oriented are least knowledgeable, all mean values are located on a 5-point rating scale from 1 (disagree) to 5 (I totally agree).

Future research should further explore the influence of different income levels as well as ethnicity on online privacy literacy. Another aspect about online privacy literacy that could be further differentiated is the extent to which Germans from variating demographic backgrounds actually read through privacy policies such as cookies, and on another note, whether Germans understand data laws that apply in their country.

7. Attitudes Towards Data Receiver

In the following, the overview of results regarding underlying attitudes towards data receivers in Germany is split into attitudes towards governments and attitudes towards companies.

a. Attitudes Towards Governments

Generally speaking, trust in the national government (37%) is low in Germany, while trust in foreign governments (12%) is even lower. Therefore, distrust in governments' correct use of collected data appears to be rather high in Germany (61.5%). Overall, both national (64%) and foreign governments (68%) contribute to general distrust of the Internet.

Further research is needed regarding whether Germans generally call for stronger governmental regulations and whether they hope to feel more secure in disclosing data when being more protected in their actions. Additionally, it would be rewarding to investigate the link between a person's political orientation and the resulting attitudes towards governmental surveillance and regulations.

b. Attitudes Towards Companies

From the user's point of view, companies do not appear to be trustworthy (71.6%) in fulfilling their task to protect disclosed information. In comparison, more respondents (51%) believe that major companies make enough of an effort than governments (41%). Depending on which industry a firm operates in, confidence can vary. A majority of respondents believes healthcare providers (56%) to be trustworthy, yet only minorities believe the same for financial service companies (38%), shipping companies (34%), Social Media sites (15%) and media companies (17%). 68% of surveyed Germans indicate that companies in general have added to their distrust in the Internet, 80% of Germans state that online firms and specifically social media companies (74%) increase their privacy concerns. Further contributors to distrust in the Internet are search engines (64%), Internet Service providers (55%), e-commerce platforms (57%) and online and mobile banking platforms (44%).

8. Communication on Data Use

Brands that process data transparently gain consumers' trust more easily. 63% of Germans indicate to feel more comfortable about disclosing private information to companies that are open about how the disclosed information will be used. More than half of the participants (55%) state to feel more at ease about data disclosure as long as companies promise to not sell their information to third parties.

XII. References

CIGI-Ipsos (2019a). CIGI-Ipsos Global Survey on Internet Security and Trust. Parts I & II: Internet Security, Online Privacy & Trust. Centre for International Governance Innovation. www.cigionline.org/internet-survey-2019 (last access: 01/30/2022).

CIGI-Ipsos (2019b). CIGI-Ipsos Global Survey Internet Security & Trust. Part 6: Cross-Border Data Flows. Centre for International Governance Innovation. www.cigionline.org/internet-survey-2019 (last access: 01/30/2022).

CIGI-Ipsos (2019c). CIGI-Ipsos Global Survey on Internet Security & Trust. Detailed Results Tables. www.cigionline.org/internet-survey-2019 (last access: 01/30/2022).

DLA Piper (2021). Data Protection Laws of the World: German – Definition of Personal Data. https://www.dlapiperdataprotection.com/index.html?t=definitions&c=DE&c2= last access: 12/14/2021).

EVS/WVS (2021a). World Values Survey Wave 7 (2017-2020). Questionnaire: WVS-7 Master Questionnaire 2017-2020. https://www.worldvaluessurvey.org/WVSDocumentationWV7.jsp (last access: 12/15/2021).

EVS/WVS (2021b). European Values Study and World Values Survey: Joint EVS/WVS 2017-2021 Dataset (Joint EVS/WVS). JD Systems Institute & WVSA. Dataset Version 1.1.0. Citation for Data. doi: 10.14281/18241.14. https://www.worldvaluessurvey.org/WVSEVSjoint2017.jsp (last access: 12/15/2021).

EVS/WVS (2021c). European Values Study and World Values Survey: Joint EVS/WVS 2017-2020 Data-Set (version 2.0.0). Documentation: Frequency Tables. WVS/EVS Joint v2.0 Results by Country. https://www.worldvaluessurvey.org/WVSEVSjoint2017.jsp (last access: 12/15/2021).

Globe (2020). An Overview of the 2004 Study: Understanding the Relationship Between National Culture, Societal Effectiveness and Desirable Leadership Attributes. https://globeproject.com/study_2004_2007#theory (last access: 01/30/2022).

Herbert, F., Schmidbauer-Wolf, G. and Reuter, C. (2020). Differences in IT Security Behavior and Knowledge of Private Users in Germany. Wirtschaftsinformatik (Community Tracks). 168-184.

IMD (2021). IMD World Digital Competitiveness Ranking 2021. https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/ (last access: 01/30/2022).

Ipsos (2019). Global Citizens & Data Privacy: An Ipsos-World Economic Forum Project. https://www.ipsos.com/sites/default/files/ct/news/documents/2019-01/ipsos-wef_-_global_consumer_views_on_data_privacy_-_2019-01-25-final.pptx_lecture_seule_0.pdf?mod=article_inline (last access: 01/30/2022).

Jourard, S.M, Lasakow, P. (1958). Some Factors in Self-disclosure. Journal of Abnormal Psychology 56(1). 91-98. https://doi.org/10.1037/h0043357 (last access: 1/30/2022).

Kessel, L. (2022). Cultural Influences on Personal Data Disclosure Decisions: US-American Perspectives. University of Passau Institute for Law of the Digital Society Research Paper Series 22(4). 1-29. https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4068964 (last access: 03/30/2022).

Kowalewski, Sylvia, et al. (2015). Like us on Facebook! Analyzing User Preferences Regarding Privacy Settings in Germany. Procedia Manufacturing 3. 815-822.

Morey, T., Forbath, T. and Schoop, A. (2015). Customer Data: Designing for Transparency and Trust. Harvard Business Review 93.5. 96-105.

Rössler, Beate (2001). Der Wert des Privaten. Frankfurt am Main: Suhrkamp.

Trepte, S. and Masur, P. (2016). Cultural Differences in Social Media Use, Privacy, and Self Disclosure. http://opus.unihohenheim.de/volltexte/2016/1218/pdf/Trepte_Masur_ResearchReport.pdf (last access: 01/30/2022).

Trepte, S. and Masur, P. (2017). Privacy attitudes, perceptions, and behaviors of the German population. https://www.philippmasur.de/documents/pubs/Trepte_Masur_2017_Research_Report_Hohenheim.pdf (last access: 01/30/2022).

Schenk, M., Niemann, J., Reinmann, G., Schnurr, J. M., Jandt, S., and Roßnagel, A. (2012). Gläserne Freunde? Kompaktversion zur LFM-Studie Digitale Privatsphäre. Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen. Landesanstalt für Medien Nordrhein-Westfalen.

Wawra, D. (2022). The Cultural Context of Personal Data Disclosure Decisions. University of Passau Institute for Law of the Digital Society Research Paper Series 22(2). 1-19. https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4048250 (last access: 03/03/2022).

Appendix 1. List of included studies and study details

Study	Overview	Sample size	Demographics
CIGI-Ipsos Global Survey on Internet Security and Trust Part I/II (CIGI-Ipsos , 2019a)	The survey examines how privacy concerns have increased around the world and how distrust in the Internet affects global citizens in their use of the Internet. Moreover, the survey evaluates reasons for increasing privacy concerns and factors that contribute to distrust in the Internet.	N ≈[20] 1000	Age of respondents: 16 - 64 Online population
CIGI-Ipsos Global Survey Internet Security & Trust Part 6: Cross-Border Data Flows (CIGI-Ipsos, 2019b, 2019c)	The survey observes awareness of data protection and privacy rules, attitudes towards cross-border data flows, secure data storage, governmental and corporate ability to protect data.	N ≈[21] 1000	Age of respondents: 16 - 64 Online Population
Global Citizens and Data Privacy Study, Ipsos & World Economic Forum (Ipsos 2019)	The survey tracks public understanding as well as actual acceptance of new technologies around the globe.	N ≈[22]1000	Age of respondents: 16 - 64
Cultural Differences in Social Media Use, Privacy, and Self-Disclosure (Trepte & Masur 2016)	The report presents results on social media use, self-disclosure, privacy perceptions and attitudes, and privacy behavior in online environments from a cross-cultural survey.	N = 884	Average age: 24 Men 27.6%, Women: 72.4% No education: 0.1% Middle school: 0.2% In firm training: 4.1% University entrance certificate: 62.2% Bachelor: 15.9% Master: 13.9% PHD: 2.1%

[20] Indicates an approximate amount of survey respondents. Survey institutes state that the surveyed individuals were "weighted to match the population in each economy surveyed. The precision of Ipsos online polls is calculated using a credibility interval. In this case, a poll of 1,000 is accurate to +/- 3.5 %age points" (CIGI-Ipsos 2019a, p. 4).

[21] Indicates an approximate amount of survey respondents. Survey institutes state that the surveyed individuals were "weighted to match the population in each economy surveyed. The precision of Ipsos online polls is calculated using a credibility interval. In this case, a poll of 1,000 is accurate to +/- 3.5 %age points" (CIGI-Ipsos 2019a, p. 4).

[22] Indicates an approximate amount of survey respondents. The survey institute state that "precision of Ipsos online polls is calculated using a credibility interval with a poll of 1,000 accurate to +/- 3.5 %age points and of 500 accurate to +/- 5.0 %age points" (Ipsos 2019, p. 21).

Study	Overview	Sample size	Demographics
Privacy attitudes, perceptions, and behaviors of the German population (Trepte & Masur 2017)	As part of a larger study (Privatheit im Wandel), this report looks at changes in privacy behavior and data disclosure attitudes in Germany.	N = 3278	Men: 48.4% Women: 51.6% 24 years and younger: 5% 25 - 39 years: 12.4% 40 - 54 years: 23.3% 55 - 69 years: 34.6% 70 years and older: 24.7%
World Values Survey (EVS/WVS 2021)	The cooperation between the European- and the World Values Survey investigates values that are most important to people from different national backgrounds, including values that relate to attitudes towards data disclosure.	N = 2178	Age of respondents: 18+ "random probability representative samples of the adult population" (EVS/WVS 2021).
Differences in IT Security Behavior and Knowledge of Private Users in Germany (Herbert et al. 2020)	The report focuses on scrutinizing general IT and security knowledge in Germany and further looks at the link between socio-demographic details (gender, age, education, political orientation) and security knowledge and applied measures.	N = 1219	Age: 14 - 87 Women: 52% Men: 48%
Like Us on Facebook! Analyzing User Preferences Regarding Privacy Settings in Germany (Kowalewski et al. 2015)	The paper analyzes privacy competencies, knowledge, feelings of control in connection to socio-demographic details among German SNS users.	N =110	Mean age: 30.5 years Younger group (20-30 years): 54 Older group (30-66 years): 56 Women: 58 Men: 52
Gläserne Freunde?. Kompaktversion zur LFM-Studie Digitale Privatsspähre. Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen (Schenk et al. 2012)	This report is part of a larger study (Digitale Privatsspähre. Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen) and gives an overview about how young Germans perceive SNS sites, what they share online and how their behavior can affect their and others' privacy.	N ≈ 1301	