IRDG Institut für das Recht der digitalen Gesellschaft

UNIVERSITY OF PASSAU Faculty of Law

UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES NO. 22-09

CULTURAL INFLUENCES ON PERSONAL DATA DISCLOSURE DECISIONS

Chinese Perspectives

Daniela Wawra, Katharina Kindsmüller, Memoona Tawfiq, Vanessa Vollenschier, Franziska Walbert, Lisa Woldrich

March 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

Daniela Wawra is professor of linguistics and cultural studies at the University of Passau. The co-authors are student assistants. They work together in an interdisciplinary research team that explores the disclosure of personal data from a legal, cultural studies and information systems perspective.

Abstract

This paper gives an overview of survey findings from China on central parameters that can influence people's willingness to share (WTS) personal data. It provides insights into Chinese mentalities with regard to data disclosure on a macro level and thus into the cultural preconditions of information governance. This 'country report' is one of several that have been compiled in the interdisciplinary 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 Institute for Digital Transformation[2].

Cite as

Wawra, D. et al. (2022). Cultural Influences on Personal Data Disclosure Decisions – Chinese Perspectives. *University of Passau Institute for Law of the Digital Society Research Paper Series No. 22-09*. https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/.

Keywords

Culture, China, Data Disclosure, Digitalization, 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

This paper 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 Chinese 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 China. Our approach can be characterized as a macro level analysis (cf. Wawra 2022). We have composed similar 'reports' for other countries in our project[3], 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] The first report that has been developed in our project focuses on the US context (cf. Kessel 2022).

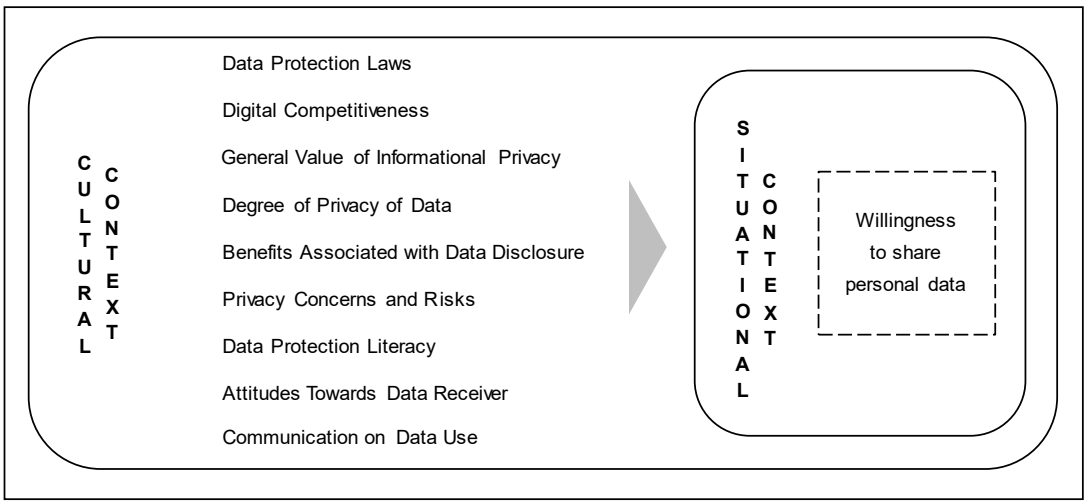

Fig. 1. Central parameters of data disclosure (from Wawra 2022).

II. Selected Survey Data

This report summarizes relevant findings primarily from large recent cross-national surveys on informational privacy, data control, data protection, and data disclosure in China. The sample size was usually 1000 or more, once there were about 200 and once 80 respondents. Appendix 1 provides an overview and details of the surveys included, such as sample size and demographic information on respondents.

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).[4] *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 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).*[5]

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

[5] The paragraph from "Specifically […]" to "transformation […]" has been added in all country reports and has been adopted literally from the first country report (Kessel 2022).

For its overall performance, China is ranked 15th out of 64 countries in 2021 for digital competitiveness. China receives the 6th rank for its advances in **knowledge**, rank 20 in the category **technology**, and 17 in **future readiness** for digitization. When looking at the five-year development, China's rankings have improved considerably: Overall (from 31st in 2017 to 15th in 2021), as well as in the categories **knowledge** (from 23rd in 2017 to 6th in 2021), **technology** (from 36th in 2017 to 20th in 2021), and **future readiness** (from 34th in 2017 to 17th in 2021) (cf. IMD 2021, p. 66).

Subfactor rankings with regard to **knowledge** position China 12th in the subcategory **talent** and 16th for personnel's digital and technological skills, which is one of the items of this category. China is 35th in the subcategory **training and education** and 1st in **scientific concentration**[6] (cf. IMD 2021, p. 67).

In the field of **technology**, China ranks 15th in the subcategory of **regulatory framework** and 16th for starting a business as well as development & application of technology, two of the items of this subcategory. For the subfactor **capital**, China occupies 27th place and ranks 16th for funding for technological development. It ranks 28th for the subfactor **technological framework**[7], and here 13th for communications technology (cf. IMD 2021, p. 67).

In terms of **future readiness**, China ranks 19th for the subfactor **adaptive attitudes**, 3rd for **business agility** and 32nd for **IT integration**. In the subcategory of adaptive attitudes, it ranks 9th for e-participation[8], and 17th for smartphone possession. In the subcategory of business agility, it occupies 11th place with regard to the use of big data and analytics. In the final subcategory of IT integration its ranks are 40th for e-government[9] and 12th for cyber security (cf. IMD 2021, p. 67).

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 China consider this demand].[10]

The following surveyed questions allow for conclusions in this respect. The World Values Survey (cf. EVS/WVS 2021a, b) has asked Chinese people to assess the governmental collection of personal data in terms of surveillance. A solid majority of Chinese respondents approve of governmental video surveillance in public: 82% agree that their government should have this right (cf. EVS/WVS 2021c, p. 427) (Fig. 2).

---

[6] The subcategory "scientific concentration" comprises the items "Total expenditure on R&D (%) (Percentage of GDP)" (R&D=Research and Development), "Total R&D personnel per capita (Full-time work equivalent (FTE) per 1000 people)", "Female researchers (% of total (headcount FT&PT))", "R&D productivity by publication (No. of scientific articles over R&D expenditure (as % GDP))", "Scientific and technical employment (% of total employment)", "High-tech patent grants (% of all patents granted by applicant's origin (average 2014-2016))", and "Robots in Education and R&D (number of robots)" (IMD 2021, p. 180).

[7] The subcategory "technological framework" includes the items "Communications technology" (IMD 2021, p. 105), "Mobile broadband subscribers (4G & 5G market, % of mobile market)", "Wireless broadband (Penetration rate (per 100 people))", "Internet users (Number of Internet users per 1000 people)", "Internet bandwidth speed (Average speed)" and "High-tech exports (%) (Percentage of manufactured exports)" (IMD 2021, p. 181-182).

[8] "Use of online services that facilitate public's interaction with government" (IMD 2021, p. 182).

[9] "Provision of online government services to promote access and inclusion of citizens" (IMD 2021, p. 183).

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

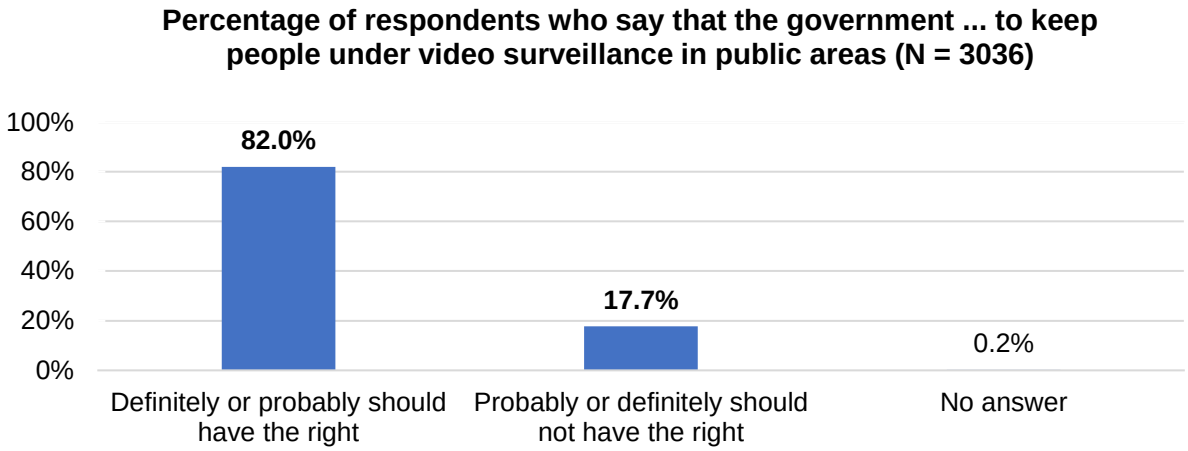

Fig. 2. Respondents' attitudes towards video surveillance by their government (cf. EVS/WVS 2021c, p. 427).

Additionally, a majority (60.6%) of Chinese respondents agree that their government should be allowed to monitor emails and other information that is exchanged online (cf. EVS/WVS 2021c, p. 429) (Fig. 3).

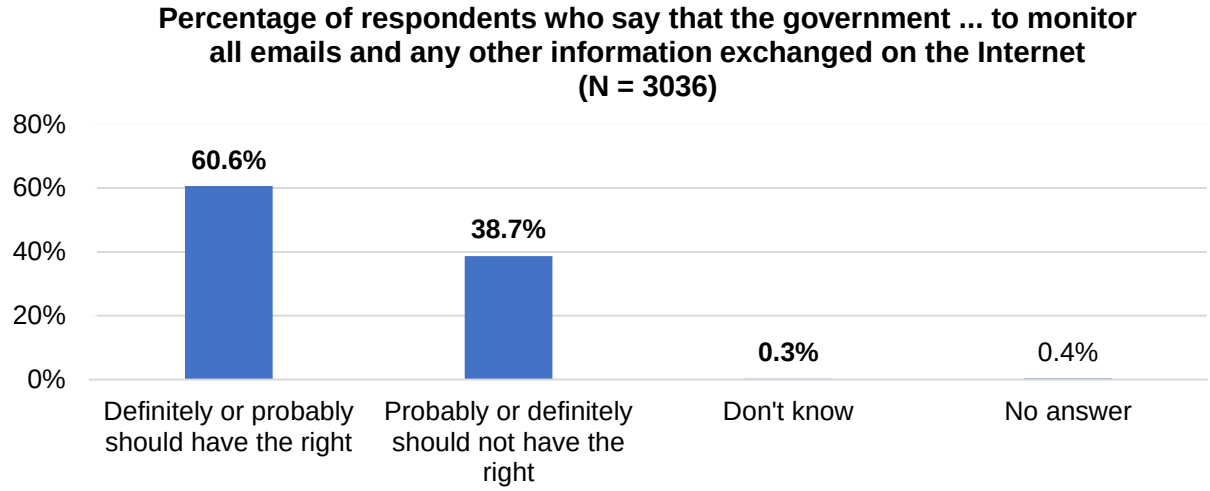

Fig. 3. Respondents' attitudes towards email and Internet monitoring by their government (cf. EVS/WVS 2021c, p. 429).

Chinese respondents are also slightly in favor (52.8%) that their government should have the right to collect data on anyone living in China without their knowledge (cf. EVS/WVS 2021c, p. 431) (Fig. 4).

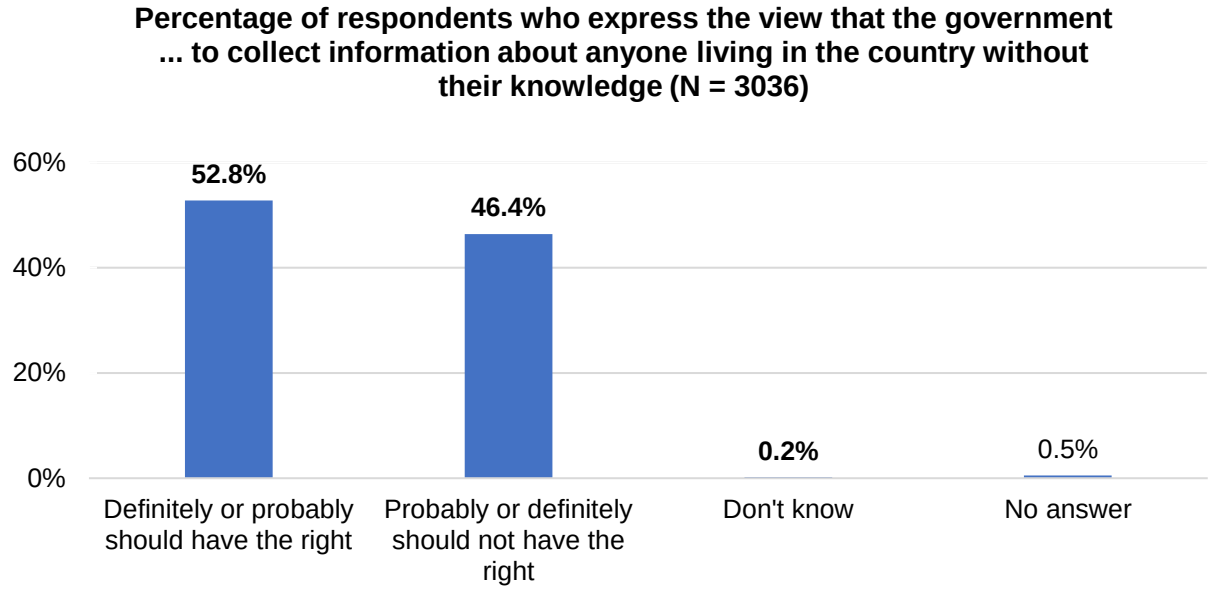

Fig. 4. Respondents' views on data tracking by the government without consent (cf. EVS/WVS 2021c, p. 431).

Surveillance at work is accepted by almost half (47%) of the respondents from China, who report that they do not mind if their employer uses technology, like sensors and wearable devices, to monitor their performance. 44% are not opposed to their employer having access to their personal data like their social media profile (cf. PwC 2021, p. 35).

With regard to the use of collected personal data by companies, 57% of Chinese respondents somewhat or strongly agree that consumers should be able to refuse this. Furthermore, 68% believe that consumers should be paid or rewarded if they allow companies to use their data. However, nearly half (49%) of the respondents from China do not mind if companies use collected data (cf. Ipsos 2019, p. 12) (Fig. 5).

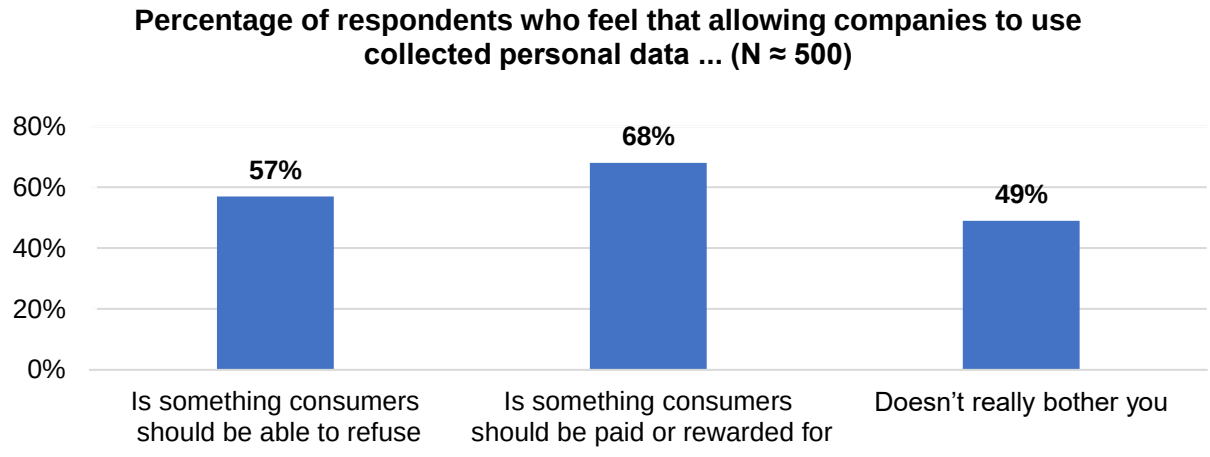

Fig. 5. Attitudes towards being able to refuse the use of collected data by companies or being paid/rewarded (cf. Ipsos 2019, p. 12).

V. Degree of Privacy of Data

[This] parameter […] surveys how private or sensitive […] certain kinds of personal data [are for Chinese respondents].[11]

For an indication of what types of personal data are considered particularly private in China, let us take a look at their legal definition. However, "[t]here is no single, pervasive definition of personal data […], but the concept of personal data in the various laws, regulations and guidance that comprise the data protection framework in [China] […] are starting to become more aligned" (DLA Piper 2021). From this data protection framework, the following approximation to a definition can be excerpted:

"[P]ersonal data (which is generally referred to as 'personal information' […]) means all kinds of information (including sensitive personal information) recorded by electronic means or otherwise that can be used to independently identify or be combined with other information to identify a natural person's information" (DLA Piper 2021).

The Personal Information Protection Law of the People's Republic of China (Chapter I, Article 4)[12] explicitly excludes "anonymized information" from this definition. A "single, pervasive definition […] for sensitive personal data (which is generally referred to as "sensitive personal information" […]") is also missing. The PIS [Personal Information Security] Specification, however, an amendment to China's Cybersecurity Law, distinguishes "between sensitive personal information and general personal information". Sensitive personal information includes "personal identification number, mobile phone number, individual biometric information, bank account number, correspondence records and contents, property information, credit information, location tracking, lodging information, health and physiological information and transaction information" (DLA Piper 2021). Moreover, the Personal Information Protection Law of the People's Republic of China (Chapter II, Section 2, Article 28)[13] defines sensitive personal information as "personal information that once leaked or illegally used, may easily lead to the infringement of the personal dignity of a natural person or may endanger his personal safety or property". It includes "information such as biometrics, religious belief, specific identity, medical health status, financial accounts, and the person's whereabouts, as well as the personal information of a minor under the age of 14 years".

Trepte and Masur (2016) surveyed "the extent to which [different kinds of behaviors and information] have the potential to affect [Chinese respondents'] privacy" (1 means "does not affect my privacy at all", 5 "affects my privacy very much") (Trepte and Masur 2016, pp. 61-62). Respondents from China show a slightly more than medium sensitivity with regard to revealing their relationship status (2.97), their political orientation (2.69), and their sexual orientation (2.62). Only having an open profile is a more sensitive issue (3.33) (cf. Trepte and Masur 2016, p. 62). Trepte and Masur (2016) also surveyed the sensitivity of specific data in more detail. For this, they adapted a scale from Jourard and Lasakow (1958). The items that were surveyed go beyond the legal categories of sensitive personal information. Figure 6 gives an overview of the results of their study:

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

[12] http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (last access: 03/07/2022).

[13] http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (last access: 03/07/2022).

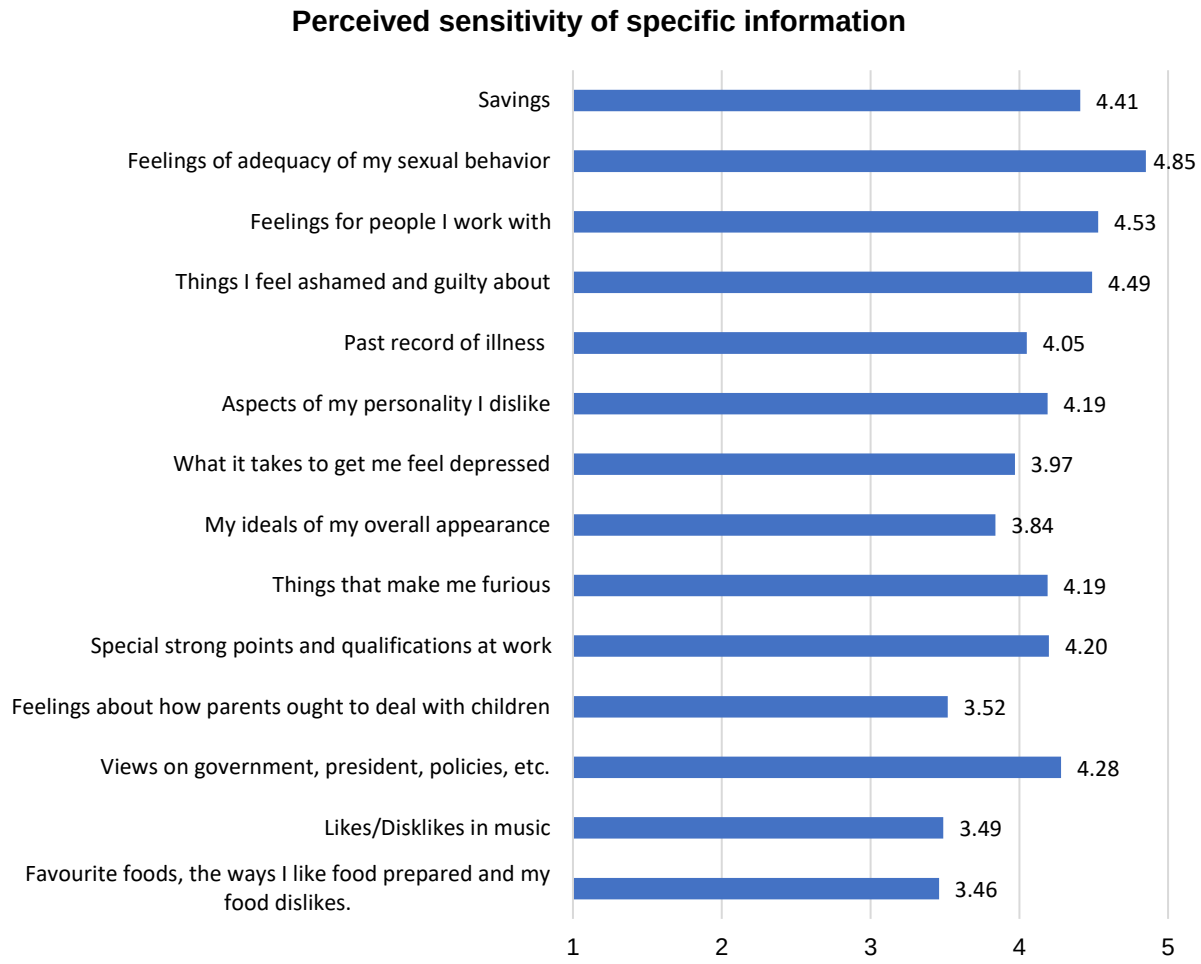

Fig. 6. Perceived sensitivity of information (1 = not at all sensitive to 7 = very sensitive) (cf. Trepte and Masur 2016, p. 63).

The results of the survey show that Chinese respondents are most sensitive about information on their "feelings of adequacy" of their "sexual behavior" (4.85), their real feelings for people they work with (4.53) and what they "feel ashamed and guilty about" (4.49) (cf. Trepte and Masur 2016, p. 63) (Fig. 6).

VI. Benefits Associated with Data Disclosure

[This] parameter […] renders the positive effects [Chinese respondents] expect from the disclosure of their personal data.[14]

Almost two thirds of Chinese respondents (64%) believe that sharing personal data with companies makes it easier for them to offer customers better information, products, and services for their individual needs. The same percentage of participants in the survey (64%) think that it makes it easier for them as consumers too, to find relevant information, products, and services. 63% indicate that the disclosure of personal data to companies can help them (as consumers) save time, and 60% agree that it can help them save money (cf. Ipsos 2019, p. 12) (Fig. 7).

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

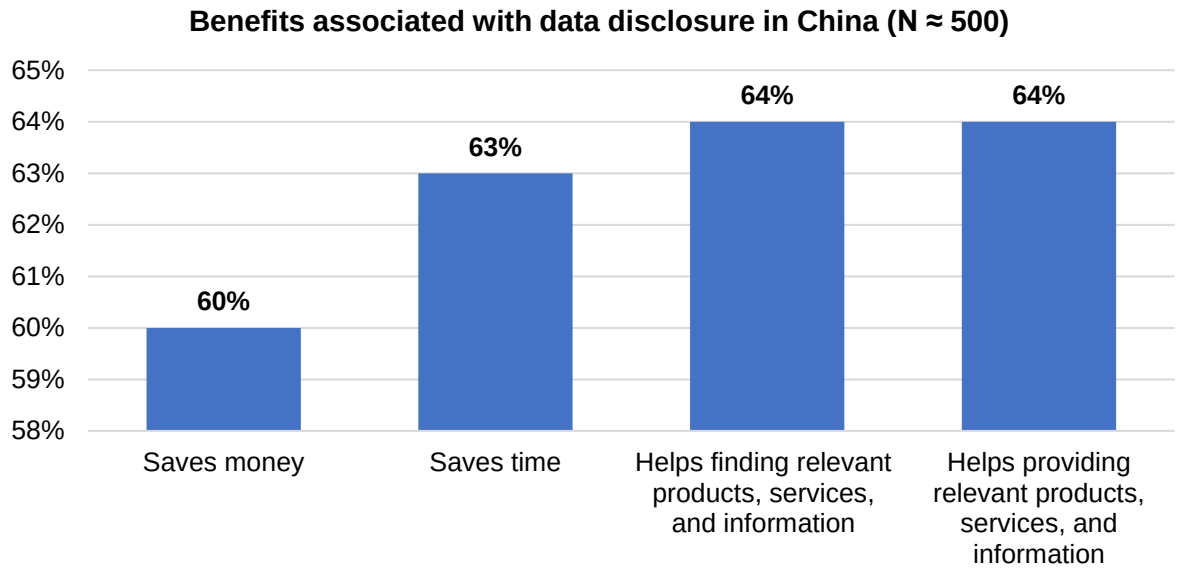

Fig. 7. Benefits associated with data disclosure in China (cf. Ipsos 2019, p. 12).

Asked directly whether they would be "willing to share […] personal data (health, financial, driving records, energy use, etc.) in exchange for benefits or rewards like lower costs or personalized service" (GfK 2017), on a seven-point Likert scale (1 meaning they don't agree at all, 7 they agree completely), 38% of Chinese respondents indicate six- or seven-point agreement (cf. GfK 2017, p. 74).

VII. Privacy Concerns and Risks

[This] parameter […] comprises the negative effects [Chinese respondents] associate with data disclosure. These include their general concerns about the security of their personal data, and their control over them.[15]

1. Concerns and Risks related to Data Security

Ipsos (2019) provides no data for China with regard to the question whether people feel more comfortable with sharing their data with companies that have "never been subject to any breach, leak, or fraudulent usage of data" (Ipsos 2019, p. 14). Neither was the question surveyed in China if people want their "online data & personal information" to be "stored on a secure server", preferably "in their own economy" (CIGI-Ipsos 2019b, pp. 13, 15) or abroad, and whether they care if their data left China (CIGI-Ipsos 2019b, pp. 17, 19).

In a survey by YouGov, however, a majority of Chinese respondents (52%) indicate that they value the security of an app more than its functionality and convenience (cf. Bruce 2021).

2. Concerns and Risks related to Data Control

In a study by Trepte and Masur (2016, p. 40) participants were asked "to rate how likely they thought having an open profile would lead to various negative consequences (e.g. increasing the chances of data abuse, increasing the chances of unwanted advances, increasing the chances of being damaged by gossip)" (1 meaning "not likely at all", 5 meaning "very likely"). Another survey question asked about whether respondents thought that uploading pictures could have negative consequences (cf. Trepte and Masur 2016, p. 41). Both are considered to be quite risky by Chinese

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

respondents, the results being 3.96 for an open social media profile and 3.91 for the uploading of pictures (cf. Trepte and Masur 2016, pp. 40, 41).

In addition, a majority of Chinese respondents report that they disclose less personal data online (60%) because they do not trust the Internet. Almost a third of the respondents says they put more effort into securing their devices (30%). A minority uses the Internet more selectively (25%), self-censors what they say online (21%), or makes fewer online purchases (12%) as a consequence of their distrust of the Internet, according to their self-report (cf. CIGI-Ipsos 2019c, p. 24) (Fig. 8).

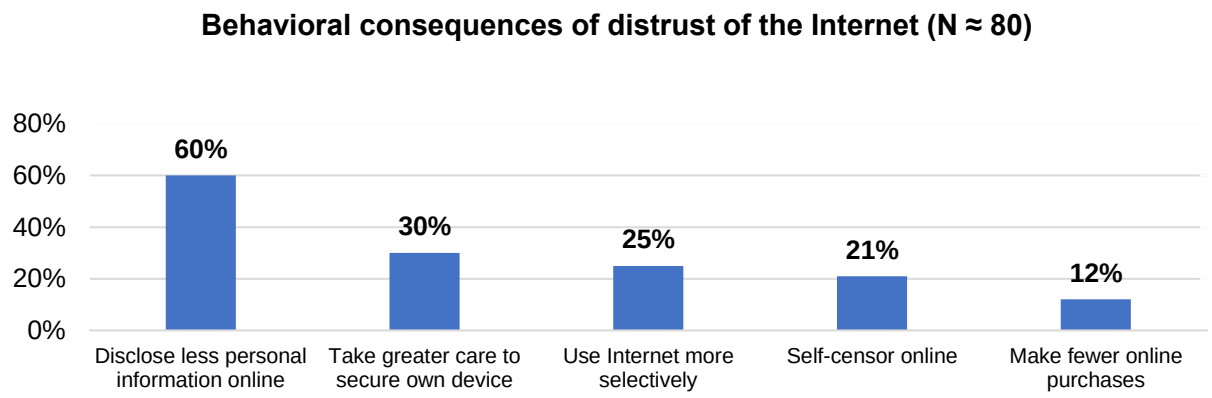

Fig. 8. Behavioral consequences of distrust of the Internet (cf. CIGI-Ipsos 2019c, p. 24).

VIII. Data Protection Literacy

[Data Protection Literacy] captures [Chinese people's] 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.[16]

Almost half (46%) of Chinese respondents say that they are very or somewhat aware of the data protection and privacy rules of their country, while a majority (54%) reports that they are not very or not at all aware of them (cf. CIGI-Ipsos 2019b, p. 8, 2019c, p. 281) (Fig. 9).

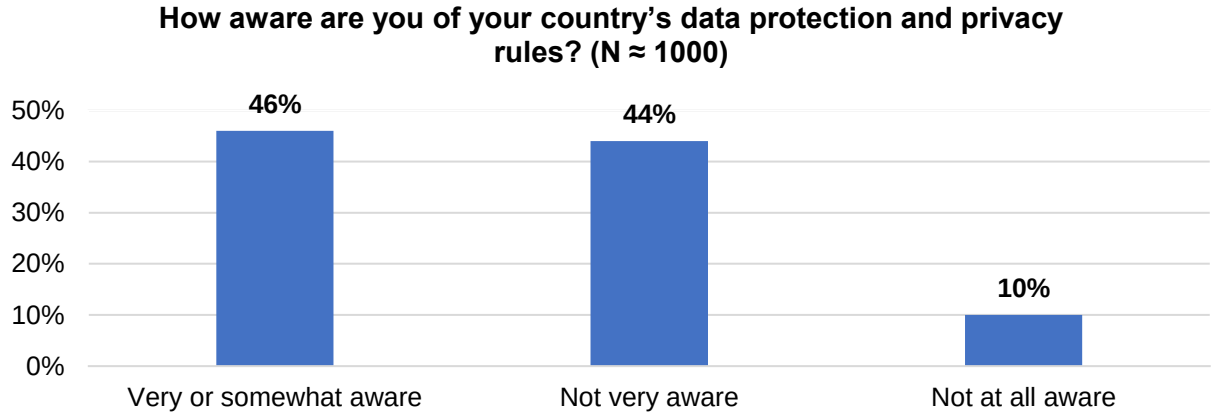

Fig. 9. Awareness of data protection and privacy rules in China (cf. CIGI-Ipsos 2019c, p. 281).

In another study, the percentage of Chinese respondents who say they are aware of privacy laws is lower, with only a third of them (33%) reporting this (cf. Cisco 2021, p. 11). A solid majority (77%)

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

of respondents from China, who said they knew the law, attribute a positive effect to China's Cyber Security Law (CSL) (only 3% expect a negative effect, 20% are neutral) (cf. Cisco 2021, p.10).

CIGI-Ipsos does not have data for China for the item whether respondents agree that they themselves do enough to protect their data (CIGI-Ipsos 2019b, p. 29, 2019c, p. 283).

IX. Attitudes Towards Data Receiver

[This] parameter […] refers to [Chinese people's] 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.[17]

Trust towards others is rather high among Chinese respondents. A majority (63.5%) feels that most people can be trusted (cf. EVS/WVS 2021a, p. 7, 2021c, p. 174) (Fig. 10).

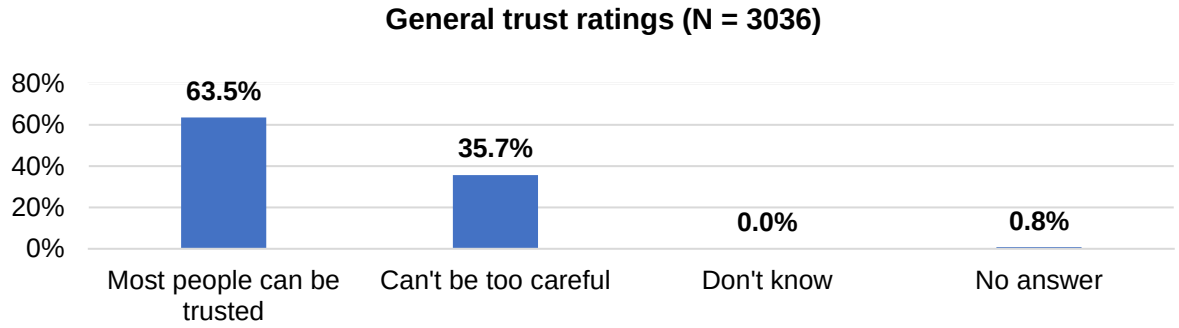

Fig. 10. Trust towards others in China (cf. EVS/WVS 2021c, p. 174).

This general trust towards others could influence Chinese people's data disclosure decisions. The following chapters provide more detailed insights into respondents' attitudes towards governments and companies.

1. Attitudes Towards Governments

Chinese people's attitudes towards their government and other political institutions reflect the prevailing general trust towards others. A great majority of respondents report that they trust their government (94.6%), political parties (90.5%), and parliament (92.2%) (cf. EVS/WVS 2021c, pp. 266, 273, 275) (Fig. 11).

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

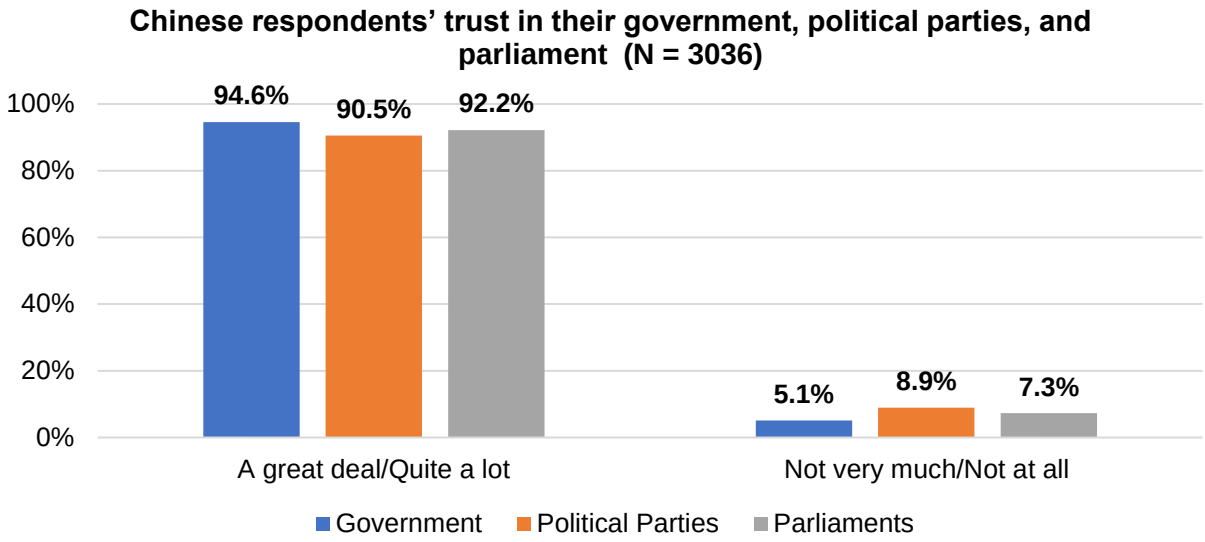

Fig. 11. Chinese respondents' trust in their government, political parties, and parliament (cf. EVS/WVS 2021c, pp. 266, 273, 275).

Only a minority, i.e. 44% of the respondents from China, trust foreign governments, however, that they use collected data correctly (cf. Ipsos 2019, p. 20). CIGI-Ipsos does not provide data for China with regard to the question whether respondents think that their own government uses their personal data correctly (cf. Ipsos 2019, p. 20). Neither does CIGI-Ipsos (2019b, p. 45) have data for China concerning the question whether they consider their government's efforts to protect their data as sufficient. Furthermore, CIGI-Ipsos (2019a, p. 117, 119, 2019c, p. 20) did not survey Chinese people's opinions on whether their government or foreign governments contribute to distrust of the Internet.

2. Attitudes Towards Companies

CIGI-Ipsos (2019c, p. 283) does not provide data for China with regard to the question how much trust people have in companies that they do enough to protect their data.

As the Ipsos survey shows, however, Chinese people's confidence in companies to use their data correctly is relatively high, as always more than 50% of respondents express their belief in the companies in this respect (see Fig. 12 below). Their trust varies, however, when looking at different industries: They have most confidence in healthcare providers (74%), financial services companies (69%), and telecommunications companies (67%) (cf. Ipsos 2019, p. 20) (Fig. 12).

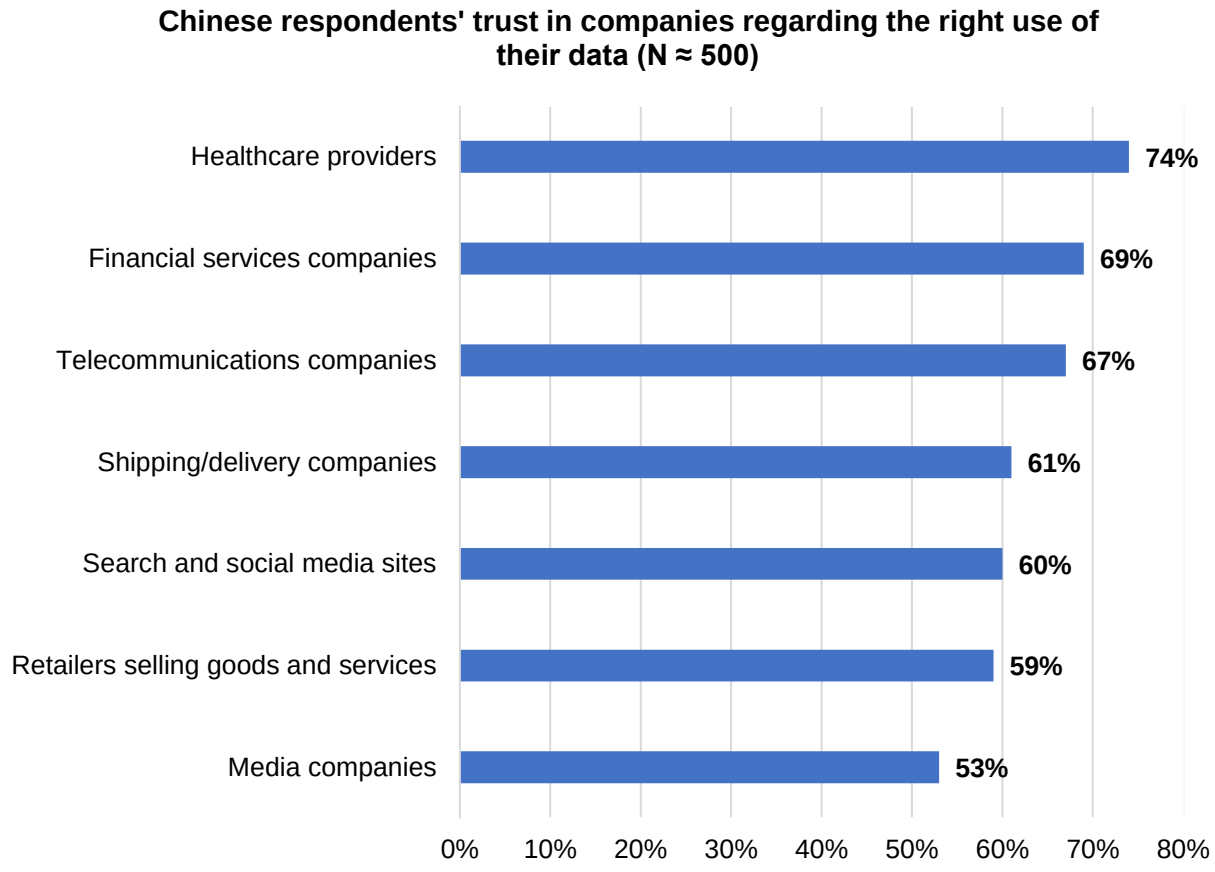

Fig. 12. Chinese respondents' trust in companies regarding the right use of their data (cf. Ipsos 2019, p. 20).

While trust in the other industries is somewhat lower, the threshold of 50% of respondents still trusting the specific type of company is never undercut. More than half of the respondents from China express their trust in shipping/delivery companies (61%), search and social media sites (60%), retailers (59%), and media companies (53%) and believe that they use their data correctly (cf. Ipsos 2019, p. 20).

At the same time, the following institutions are reported to contribute to distrust of the Internet by a majority of respondents from China: social media companies (71%), Internet service providers (63%), search engines (61%), and e-commerce platforms (56%). 43% say that online and mobile banking providers add to their lacking confidence in the Internet (cf. CIGI-Ipsos 2019c, p. 20) (Fig. 13).

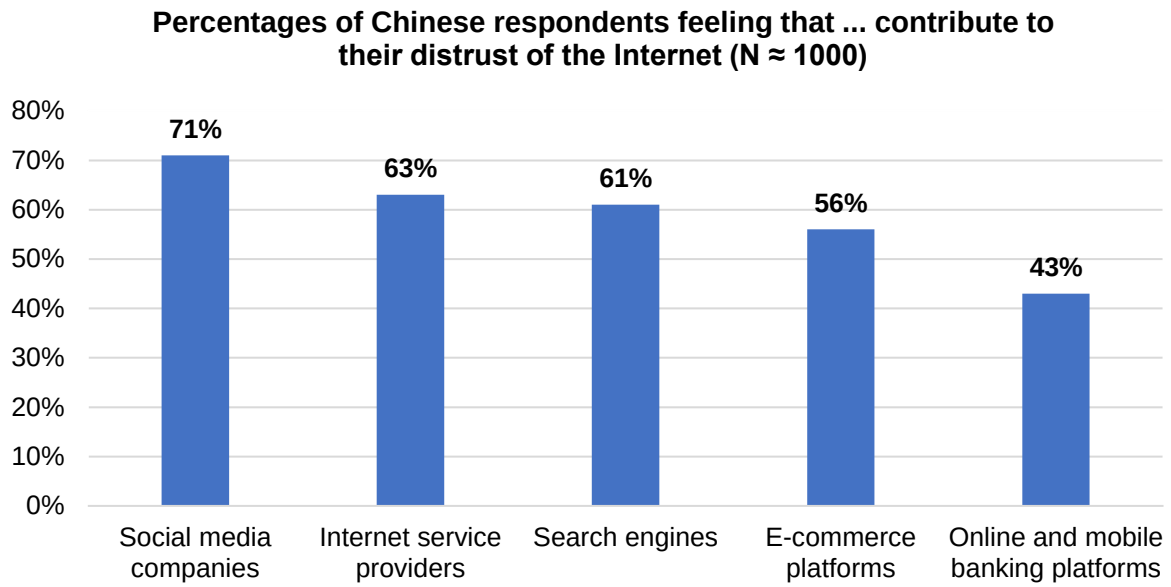

Fig. 13. Percentages of Chinese respondents feeling that the mentioned institutions contribute to their distrust of the Internet (cf. CIGI-Ipsos 2019c, p. 20).

X. Communication on Data Use

[This] parameter […] relates to the importance [Chinese respondents] attribute to communication on how their personal data are used.[18]

Ipsos (2019, p. 14) does not provide data for China with regard to the question whether people would be more comfortable giving their data to companies that communicate transparently what the data will be used for. A majority (60%) of the respondents from China report, however, that they would be most willing to share their data with companies or government institutions that clearly communicate potential risks (cf. Ipsos 2019, p. 17).

XI. Key Findings

This section summarizes and interprets the main findings of the studies presented above to allow for a quick grasp of the major outcomes of the analysis and to facilitate cross-cultural comparison. Furthermore, research gaps are identified. As far as possible, the general direction of the influence of the various factors cited below on the WTS personal data is indicated, i.e. positive (increasing) or negative (reducing) (cf. also Wawra 2022, II. 9. and IV. 2.). It should be noted that we focus on each parameter's influence on the WTS data from a macro perspective. Their individual intensity, reaching from a potentially significant to no influence at all, depends on the interplay with other cultural-contextual as well as socio-demographic (e.g. age, education, gender, income) and personality parameters in concrete situational contexts (cf. Wawra 2022, II. 9., III., IV. 3.). This has to be researched with a micro level approach. Socio-demographic factors and personality traits in particular are still under-researched in relation to Chinese people's WTS data (cf. Wawra 2022, IV. 3.).

1. Digital Competitiveness

For its overall performance, China is positioned 15th out of 64 evaluated countries in the IMD (2021) ranking for digital competitiveness. It is thus among the best quarter of all countries. Furthermore, it places at least among the best third in all three main categories that indicate a country's

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

digital competitiveness in the ranking: It occupies rank 6 for knowledge, rank 17 for future readiness for digitalization, and rank 20 for technology. It ranks first in several of the subcategories for knowledge, among them scientific concentration. In the category future readiness, it achieved third place for business agility. China is among the best 20 to about 30% of all countries in most subcategories. Its worst ranking is 35th for training and education, which means that China is still in the midfield in this subcategory. Further subcategories where this is the case are IT integration (rank 32) in the category future readiness, technological framework (rank 28), and capital (rank 27) in the category technology. The effect (of the individual components) of this parameter on people's WTS personal data has yet to be studied in detail (cf. Wawra 2022, IV. 2.).

2. General Value of Informational Privacy

It depends on the situational context and on the data receiver whether Chinese respondents consider surveillance as more or less acceptable. A majority of Chinese respondents (82%) accept governmental surveillance in public areas. Additionally, a majority approves of governmental email and Internet monitoring (60.6%) as well as secret data collection by the government in general (52.8%). Accordingly, the majority of Chinese respondents do not place a high value on informational privacy, not in online environments and even less so in the context of state surveillance in public spaces.

Surveillance at work by technological means is accepted by almost half (47%) of the Chinese respondents. 44% do not mind if their employer has access to their personal data (e.g. to their social media profile). Regarding the use of collected personal data by companies, a majority (57%) of Chinese respondents agree that consumers should have the right to refuse this. At the same time, nearly half (49%) of the respondents from China do not mind if companies use collected personal data. Even more respondents (68%) believe that consumers should be compensated for the use of their data.

This shows that informational privacy is held in high regard by a majority of Chinese respondents in the context of employer monitoring. A slight majority also value their informational privacy as consumers. In addition, a much higher percentage of Chinese respondents believe that concessions to their informational privacy in this regard are worth compensation.

3. Degree of Privacy of Data

In China, sensitive personal data are usually referred to as sensitive personal information in legal texts. Sensitive personal information is defined as information that will lead to negative consequences for an individual or 'data subject' (in the diction of the legal text) if it is disclosed or abused. It comprises

- personal identification number
- mobile phone number
- individual biometric information
- bank account number, credit information, financial accounts
- property information
- transaction information
- correspondence records and contents

- location tracking
- lodging information
- health and physiological information
- specific identity
- religious belief and
- personal information of a minor under the age of 14 years

Chinese respondents' assessments of certain personal data – which go beyond the legal categories – indicate that an open profile could affect their privacy the most (3.33) (with 1 indicating that it does not affect their privacy at all and 5 that it affects their privacy very much). A slightly more than medium privacy sensitivity shows with regard to revealing their relationship status (2.97), their political (2.69) and sexual orientation (2.62). When asked about the perceived sensitivity of certain personal data (with 1 indicating that the data are not at all sensitive and 7 that they are very sensitive), Chinese respondents express the highest sensitivity for information on their feelings, i.e. specifically for their feelings of adequacy of their sexual behavior (4.85), their real feelings for people they work with (4.53), and what they feel ashamed and guilty about (4.49).

4. Benefits Associated with Data Disclosure

As benefits of disclosing personal data, Chinese respondents say that it helps

- companies to better tailor information, products, and services to their needs (64%)
- them as consumers to find relevant information, products, and services (64%)
- them as consumers save time (63%) and money (60%).

Thus, clear majorities consider all of these as benefits of data disclosure. However, when asked directly about their willingness to disclose, only 38% of Chinese respondents said they would be very willing to share personal data (six- or seven-point agreement on a seven-point Likert scale) if they benefit or are rewarded in some way (lower costs and personalized service were given as examples but no differentiation was made). Health and financial data as well as driving records and information on energy use were mentioned as examples of personal data in the survey, it did not, however, differentiate between these different types of data either. As health and financial data are sensitive personal data according to Chinese law, and as these and financial data have also been categorized by a majority as sensitive or being above a medium privacy threshold (see Degree of Privacy of Data above), this could also explain why a majority of Chinese respondents indicate that they would not be very willing to share their data, even if they could expect a benefit: For Ackermann et al. (2021) conclude that the higher the perceived sensitivity of data, the less other variables (such as benefits of disclosure) affect people's WTS data:

"In other words, consumers will be very unlikely to share private data that they perceive as very sensitive, irrespective of what type of compensation they are offered in return or the degree of anonymity that is granted to them" (Ackermann et al. 2021).

If, however, data are

"not perceived as very sensitive, other factors, such as what compensation is offered and whether the data allow for personal identification […], will likely have a considerable impact on individual decisions to share these data" (Ackermann et al. 2021).

Further studies that distinguish between more and less sensitive types of data are needed to determine whether this also applies to Chinese data disclosure culture. Moreover, they should systematically differentiate between different kinds of benefits as there might be cultural differences with regard to which value is attributed to specific benefits, and this could influence people's WTS data accordingly. Research so far has for example differentiated between three categories of benefits: (1) "financial rewards", (2) "personalization benefits", and (3) "social adjustment benefits" (Buchwald et al. 2017). The latter have been defined as "the establishment of social identity by integrating into desired social groups" (Lu et al. 2004, p. 572), which allows individuals to "fulfil their need for affiliation" (Buchwald et al. 2017).

5. Privacy Concerns and Risks

a. Data Security

Survey data for China are still missing with regard to the question whether people feel more comfortable with sharing their data with companies that have "never been subject to any breach, leak, or fraudulent usage of data" (cf. Ipsos 2019, p. 14). Neither was the question surveyed in China if people want their "online data & personal information" to be "stored on a secure server", preferably "in their own economy" (CIGI-Ipsos 2019b, pp. 13, 15) or abroad, and whether they care if their data left China (cf. CIGI-Ipsos 2019b, pp. 17, 19).

In a survey by YouGov (Bruce 2021), however, a majority of Chinese respondents (52%) indicate that they value the security of an app more than its functionality and convenience.

b. Data Control

Having an open social media profile and uploading pictures online are considered to be quite risky by respondents from China: The probability that this would have negative consequences was rated 3.96 for an open profile and 3.91 for uploading pictures (1 indicating that negative consequences are not likely at all, 5 indicating that they are very likely).

Because of their concerns about control over their data on the Internet, a majority of Chinese respondents report that they disclose less personal information online (60%). Only about a third (30%) takes greater care to secure their devices, a quarter (25%) says they use the Internet more selectively and 21% self-censor what they say online. 12% indicate they make fewer purchases online.

Privacy concerns thus reduce the WTS data among a majority of Chinese respondents. According to previous research (cf. e.g. Hoffmann et al. 1999, Roeber et al. 2015, and Ackermann et al. 2021), people's feeling that they are in control of their personal data can be improved by providing a delete option for data and/or by guaranteeing anonymity. Ackermann et al. (2021) even identified the granting of anonymity as "the most effective single factor for evoking WTS". However, this does not seem to apply to very sensitive data (cf. Ackermann et al. 2021, see above). Surveys and more empirical studies on this aspect of data disclosure are needed, particularly also with Chinese respondents.

6. Data Protection Literacy

Depending on the survey, about a third (33%) to almost half (46%) of the respondents from China are aware of the data protection and privacy rules that apply in their country. A solid majority (77%) of those, who know the law, attribute a positive effect to China's Cyber Security Law (CSL).

Data for China are still lacking concerning the question whether citizens agree that they do enough to protect their data (cf. CIGI-Ipsos 2019b, p. 29, 2019c, p. 283).

Further studies should systematically differentiate between different aspects of data protection literacy, for one, between declarative and procedural knowledge, in order to (better) determine the effect (of the individual components) on people's WTS personal data (cf. Baruh et al. 2017, Wawra 2022, II. 2.).

7. Attitudes Towards Data Receiver

a. Attitudes Towards Governments

In general, a solid majority of Chinese respondents (63.5%) express trust towards others. Even more, 94.6% of the respondents from China report to generally have faith in their government, 90.5% say they trust political parties, and 92.2% express their trust in parliaments. However, trust in foreign governments to use collected personal data correctly, is significantly lower with only 44%. This suggests that the willingness of a large majority of Chinese respondents to disclose data to their own government is generally quite high, while it is rather low among a majority towards foreign governments.

Survey data for China are still needed on the question whether respondents think that their own government's efforts to protect their data are sufficient (cf. CIGI-Ipsos 2019b, p. 45). Neither are there data on whether the Chinese population trusts the domestic government in using their personal data correctly (cf. Ipsos 2019, p. 20). Besides, Chinese people's feelings with regard to the question if their government or foreign governments contribute to distrust of the Internet have not yet been surveyed (cf. CIGI-Ipsos 2019a, p. 117, 119, 2019c, p. 20). As Chinese respondents' self-reported trust in their government is unusually high compared to the other surveyed countries (cf. EVS/WVS 2021c, p. 266), it can be assumed that their approval ratings for their government would also be comparatively high for the more specific questions, and that most Chinese respondents would not report that their government contributes to distrust of the Internet. However, this will have to be tested in future surveys.

b. Attitudes Towards Companies

Still, survey data are lacking on the question how much trust people have in companies and their abilities to do enough to protect their data (cf. CIGI-Ipsos 2019c, p. 283).

The Ipsos survey (2019, p. 20), however, renders Chinese respondents' trust in companies with regard to the right use of personal data. A majority of Chinese respondents express their confidence towards all industries that were surveyed in this respect. Thus, 74% trust healthcare providers, 69% financial services companies, 67% telecommunications companies, 61% shipping/delivery companies, 60% search and social media sites, 59% retailers and 53% media companies.

At the same time, Chinese respondents indicate that the following institutions contribute to their distrust of the Internet: Social media companies (71%), Internet service providers (63%), search engines (61%), e-commerce platforms (56%), and online & mobile banking providers (43%).

A majority of Chinese respondents thus trust all of the industries mentioned above in principle, which should basically have a positive effect on their WTS data with these types of companies. However, a majority of respondents from China are skeptical about social media companies, Internet service providers, search engines, and e-commerce platforms in the Internet context. A basic negative impact on most people's WTS data is therefore to be expected in such data disclosure situations.

8. Communication on Data Use

Yet, there are no data for China concerning the question whether people would be more comfortable disclosing their data to companies that communicate transparently what the data will be used for (Ipsos 2019, p. 14). A majority of Chinese respondents, i.e. 60%, report, however, that they would be most willing to disclose personal data if potential risks were communicated clearly by companies or government institutions.

XII. Conclusion and Outlook

This study captures the narrower cultural context of data disclosure in China (cf. Wawra 2022, II. 8., III.). It provides an overview of Chinese respondents' perceptions of informational privacy, data protection, and data control issues pertaining to personal data disclosure from a macro perspective. It reflects the cultural preconditions of information governance in China by shedding light on the prevailing attitudes, assumptions, views, and reported behaviors of respondents from China that can influence their WTS personal data.

First of all, this study has shown where China stands in global comparison with regard to the country's digitalization. In addition, it has mainly provided statistical insights into

- the value Chinese respondents place on their informational privacy in different contexts
- what types of data are defined as sensitive personal data according to Chinese law and which data are considered more or less private or sensitive by Chinese respondents
- whether a better adaptation of information, products, and services to consumers' needs, the facilitation of finding these, as well as a potential saving of time and money, are considered to be benefits by a majority of respondents and whether expected benefits and rewards would be an incentive for a majority to disclose personal data
- the value Chinese people place on data security
- reported behavior that follows from perceived privacy concerns and risks
- Chinese people's awareness and evaluation of data protection and privacy rules
- Chinese people's general trust levels and their trust in domestic and foreign governments and different types of companies
- whether certain communicative content would make consumers feel more at ease when they are asked to share personal data.

The less basic WTS data the surveys indicate, the more effort organizations requesting personal data potentially have to put into convincing people to disclose their data anyway. This can be addressed through communication and business or political strategies aimed primarily at increasing people's trust in the data recipient and reducing privacy concerns. It should also be noted that previous research on data disclosure suggests that the degree of privacy or sensitivity of the data, the granting or denial of anonymity, and whether or not data are requested in line with an organization's mission and responsibilities are the factors that have the greatest influence on people's data disclosure decisions (see above; cf. Ackermann et al. 2021).

This study was able to reveal general tendencies of Chinese respondents' views on issues closely related to data disclosure decisions. It was also able to show the general direction of influence of most of the cited parameters on people's WTS data. In actual data disclosure scenarios, the

different variables can have a greater or lesser (to no) impact on people's final decision to share personal data. It must also be considered that, depending on the situation, in which personal data are requested, the disclosure decision is not always made through conscious deliberation, and actual behavior may differ from reported behavior (cf. e.g. Kim et al. 2015, Ackermann et al. 2021, Wawra 2022, II. 9.). The complex interplay of the many variables that can influence the WTS data – including not only cultural-contextual, but also socio-demographic factors and personality traits – has to be approached on a micro level and therefore needs to be further explored in concrete situational contexts.

XIII. References

Ackermann, K. A., Burkhalter, L., Mildenberger, T., Frey, M., and Bearth, A. (2021). Willingness to Share Data: Contextual Determinants of Consumers' Decisions to Share Private Data with Companies. Journal of Consumer Behaviour 2021. 1-12. DOI: 10.1002/cb.2012 (last access: 02/07/2022).

Baruh, L., Secinti, E., and Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review: Privacy Concerns Meta-Analysis. Journal of Communication 67(1). 26-53. DOI: 10.1111/jcom.12276 (last access: 02/07/2022).

Bruce, G. (2021). Convenience vs. Security: What Do Consumers Prioritize When Choosing Mobile Apps? YouGovAmerica May 22. https://today.yougov.com/topics/technology/articles-reports/2021/05/22/convenience-vs-security-what-do-consumers-prioriti (last access: 12/06/2021).

Buchwald, A., Letner, A., Urbach, N., and von Entreß-Fürsteneck, M. (2017). Towards Explaining the Willingness to Disclose Personal Self-Tracking Data to Service Providers. 2017 Twenty-Fifth European Conference on Information Systems (ECIS). 1-11. https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/682/wi-682.pdf (last access: 02/07/2022).

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: 12/15/2021).

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: 12/15/2021).

CIGI-Ipsos (2019c). CIGI-Ipsos Global Survey on Internet Security & Trust. Detailed Results Tables. www.cigionline.org/internet-survey-2019 (last access: 12/15/2021).

Cisco (2021). Consumer Privacy Survey. Building Consumer Confidence Through Transparency and Control. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf (last access: 12/03/2021).

DLA Piper (2021). Data Protection Laws of the World: China – Definition of Personal Data. https://www.dlapiperdataprotection.com/index.html?t=definitions&c=CN (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. 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/WVSDocumentationWV7.jsp (last access: 12/15/2021).

GfK (2017). Willingness to Share Personal Data in Exchange for Benefits or Rewards. https://cdn2.hubspot.net/hubfs/2405078/cms-pdfs/fileadmin/user_upload/country_one_pager/nl/images/global-gfk_onderzoek_-_delen_van_persoonlijke_data.pdf (last access: 01/18/2022).

Hoffmann, D., Novak, T., and Peralta, M. (1999). Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web. The Information Society 15(2). 129-139. DOI: 10.1080/019722499128583 (last access: 01/28/2022).

IMD (2021). IMD World Digital Competitiveness Ranking 2021. https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/ (last access: 12/15/2021).

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: 12/15/2021).

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: 12/15/2021).

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).

Kim, M., Ly, K., and Soman, D. (2015). A Behavioural Lens on Consumer Privacy. Behavioural Economics in Action Research Re-port Series. Toronto: Rotman School of Management, University of Toronto. https://inside.rotman.utoronto.ca/behaviouraleconomicsinaction/files/2013/09/ConsumerPrivacy-BEAR-2015-Final.pdf (last access: 02/07/2022).

Lu, Y., Tan, B., and Hui, K.-L. (2004). Inducing Consumers to Disclose Personal Information to Internet Businesses with Social Adjustment Benefits. Proceedings of the Twenty-Fifth International Conference on Information Systems. Washington DC, USA. http://repository.ust.hk/ir/Record/1783.1-57524 (last access: 02/16/2022).

PwC (2021). Hopes and Fears 2021. Mainland China Report. https://www.pwccn.com/en/consulting/people-and-organisation/hopes-fears-2021-china-report-apr2021.pdf (last access: 12/06/2021).

Roeber, B., Rehse, O., Knorrek, R., and Thomsen, B. (2015). Personal Data: How Context Shapes Consumers' Data Sharing with Organizations from Various Sectors. Electronic Markets 25(2). 95-108. DOI: 10.1007/s12525-015-0183-0 (last access: 01/28/2022).

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

Trepte, S., Masur, P. (2016). Cultural Differences in Social Media Use, Privacy, and Self-Disclosure. http://opus.uni-hohenheim.de/volltexte/2016/1218/pdf/Trepte_Masur_ResearchReport.pdf (last access: 12/07/2021).

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).

Westin, A. (2003). Social and Political Dimensions of Privacy: Social and Political. Journal of Social Issues 59(2). 431-453. https://doi.org/10.1111/1540-4560.00072 (last access: 02/14/2022).

Appendix 1. List of included surveys and survey details[19]

Study	Overview	Sample size	Demographics
Bruce, Graeme (2021). Convenience vs. Security: What Do Consumers Prioritize When Choosing Mobile Apps? YouGovAmerica May 22	"[G]lobal survey conducted in 17 […] markets set out to discover which is more important to consumers in each country - convenience or security" (Bruce 2021).	Ranging from N = 508 to N = 2019 (in 17 markets)	Age of respondents: 18+ nationally representative sample
CIGI-Ipsos Global Survey on Internet Security and Trust Part I/II (CIGI-Ipsos 2019a)	"The CIGI-Ipsos Global Survey […] [is] the world's largest and most comprehensive survey of internet security and trust, involving more than 25,000 internet users in over two dozen countries across North America, Latin America, Europe, the Middle East, Africa and the Asia-Pacific region" (CIGI-Ipsos 2019a). The survey examines privacy concerns and their consequences around the world.	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, c)	The survey explores people's awareness of data protection and privacy rules, their attitudes towards cross-border data flows, secure data storage, as well as governmental and corporate ability to protect data.	N ≈[21] 1000 for some questions N = 80 where indicated	Age of respondents: 16 - 64 Online population
Cisco (2021). Consumer Privacy Survey. Building Consumer Confidence Through Transparency and Control	"Participants were asked about their attitudes and activities regarding companies' use of their personal data, […] awareness and reaction to privacy legislation, and attitudes regarding	N = 2600 in 12 countries	Age of respondents: 18+ No information on number of respondents from China.

[19] Basic information on the CIGI-Ipsos (2019b, c) and EVS/WVS studies in the table and all the information in the footnotes was copied from Kessel (2022) and supplemented, mainly with specific information on respondents from China.

[20] Indicates an approximate amount of survey respondents. The respondents 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. The respondents 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 (2019b, p. 4).

Study	Overview	Sample size	Demographics
	artificial intelligence (AI) and automated decision making" (Cisco 2021, p. 3).		
European Values Study and World Values Survey (EVS/WVS 2021a, b, c)	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 = 3036	Age of respondents: 18+ "random probability representative samples of the adult population" (EVS/WVS 2021).
GfK (2017). Willingness to Share Personal Data in Exchange for Benefits or Rewards	An online survey conducted in 17 countries about people's willingness to disclose personal data if they benefit or are rewarded in some way.	N = 1510	"The data have been weighted to reflect the demographic composition of the online population age 15+" (GfK 2017, p. 4).
Ipsos Survey, Global Citizens and Data Privacy Study, Ipsos & World Economic Forum (Ipsos 2019)	The survey "track[s] and decode[s] public understanding and acceptance of new [digital] technologies across the globe" (Ipsos 2019, p. 2).	N ≈[22] 500	Age of respondents: 16 - 64 China has a "lower level[ ] of internet connectivity and [the data output] reflect[s] online populations that tend to be more urban and have higher education/income than the general population" (Ipsos 2019, p. 21).
PwC (2021). Hopes and Fears 2021. Mainland China Report	A survey of mainly workers' opinions in 19 countries about their current and future work situation.	N = 1511	Age of respondents: 7% 18-24 44% 25-34 32% 35-44 10% 45-54 7% 55-64

[22] Indicates an approximate amount of survey respondents. "The 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
			1% 65+ 94% full time workers 6% part time workers, self-employed business owners, students, people who work on a contract or temporary basis Gender: 50% female 50% male
Trepte and Masur (2016). Cultural Differences in Social Media Use, Privacy, and Self-Disclosure	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 = 185	Average age: 22 Men 26.5% Women 73.5% High school: 12.7% Associated degree: 0.6% Bachelor: 60.6% Master: 20% PHD: 6.1%