IRDG Institut für das Recht der digitalen Gesellschaft

UNIVERSITY OF PASSAU Faculty of Law

UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES NO. 22-11

CULTURAL INFLUENCES ON PERSONAL DATA DISCLOSURE DECISIONS

Russian 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 Russia on central parameters that can influence people's willingness to share (WTS) personal data. It provides insights into Russian 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 Research Institute for Digital Transformation[2].

Cite as

Wawra, D. et al. (2022). Cultural Influences on Personal Data Disclosure Decisions – Russian Perspectives. *University of Passau Institute for Law of the Digital Society Research Paper Series No. 22-11.* https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/.

Keywords

Culture, Data Disclosure, Digitalization, Information Governance, Privacy, Russia, 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 6
VII. Privacy Concerns and Risks 7
1. Concerns and Risks related to Data Security 7
2. Concerns and Risks related to Data Control 8
VIII. Data Protection Literacy 8
IX. Attitudes Towards Data Receiver 9
1. Attitudes Towards Governments 10
2. Attitudes Towards Companies 11
X. Communication on Data Use 13
XI. Key Findings 13
1. Digital Competitiveness 13
2. General Value of Informational Privacy 14
3. Degree of Privacy of Data 14
4. Benefits Associated with Data Disclosure 15
5. Privacy Concerns and Risks 16
a. Data Security 16
b. Data Control 16
6. Data Protection Literacy 16
7. Attitudes Towards Data Receiver 16
a. Attitudes Towards Governments 16
b. Attitudes Towards Companies 17
8. Communication on Data Use 17
XII. Conclusion and Outlook 17
XIII. References 18

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 Russian 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 Russia. 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 the 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 analyzed in separate legal country reports. Depending on the specific situational context, the parameters can vary within their 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).

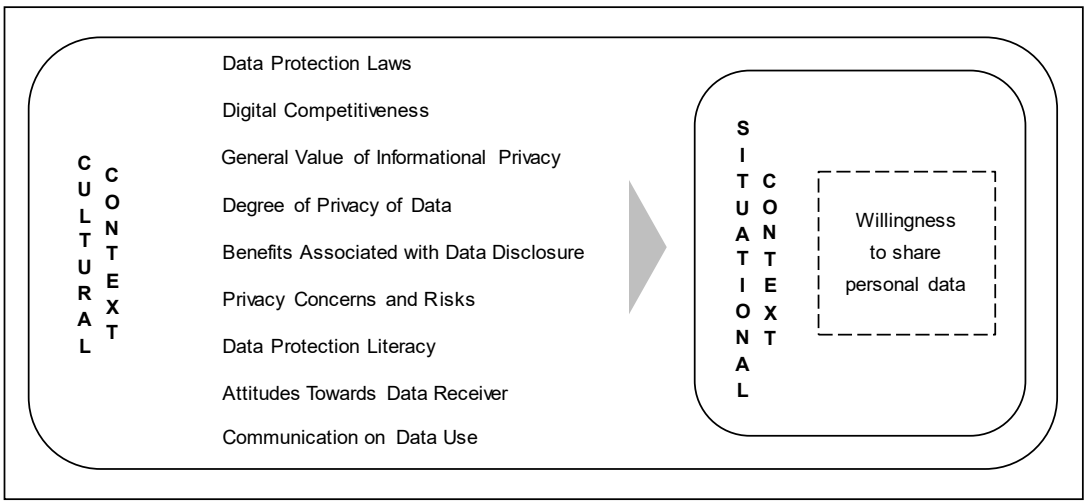

Fig. 1. Central parameters of data disclosure (from Wawra 2022).

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 Russia. The sample size was usually 1000 or more, in one survey it was 500 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, Russia is ranked 42nd out of 64 countries in 2021 for digital competitiveness. Russia receives the 24th rank for its advances in **knowledge**, rank 48 in the category **technology**, and 47 in **future readiness** for digitalization. When looking at the five-year development, Russia's rankings have been rather stable: Overall (42nd in 2017 and 2021), as well as in the category's knowledge (24th in both years), and technology, where its ranking has declined slightly (from 44th in 2017 to 48th in 2021). Its ranking for future readiness has improved a little bit (from 52nd in 2017 to 47th in 2021) (cf. IMD 2021, p. 142).

Subfactor rankings with regard to **knowledge** position Russia 44th in the subcategory **talent** and 49th for personnel's digital and technological skills, which is one of the items of this category. Russia is 6th in the subcategory **training and education**, and 24th in **scientific concentration**[6] (cf. IMD 2021, p. 143).

In the field of **technology**, Russia ranks 39th in the subcategory of **regulatory framework** and 24th for starting a business as well as 52nd for development & application of technology, two of the items in this subcategory. For the subfactor **capital**, Russia occupies 58th place and ranks 49th for funding for technological development. It ranks 45th for the subfactor **technological framework**[7], and here 26th for communications technology (cf. IMD 2021, p. 143).

In terms of **future readiness**, Russia ranks 44th for the subfactor **adaptive attitudes**, 56th for **business agility**, and 48th for **IT integration**. In the subcategory of adaptive attitudes, it ranks 26th for e-participation[8], and 29th for smartphone possession. In the subcategory of business agility, it occupies 31st place with regard to the use of big data and analytics. In the final subcategory of IT integration, its ranks are 33rd for e-government[9] and 45th for cyber security (cf. IMD 2021, p. 143).

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 Russia consider this demand].[10]

The following surveyed questions allow for conclusions in this respect.

---

[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.).

The World Values Survey (cf. EVS/WVS 2021a, b) has asked for Russians' assessment of the collection of personal data for surveillance by their government.[11] A majority of Russian respondents approve of governmental video surveillance in public: 58.6% agree that their government should have this right (cf. EVS/WVS 2021c, p. 428) (Fig. 2).

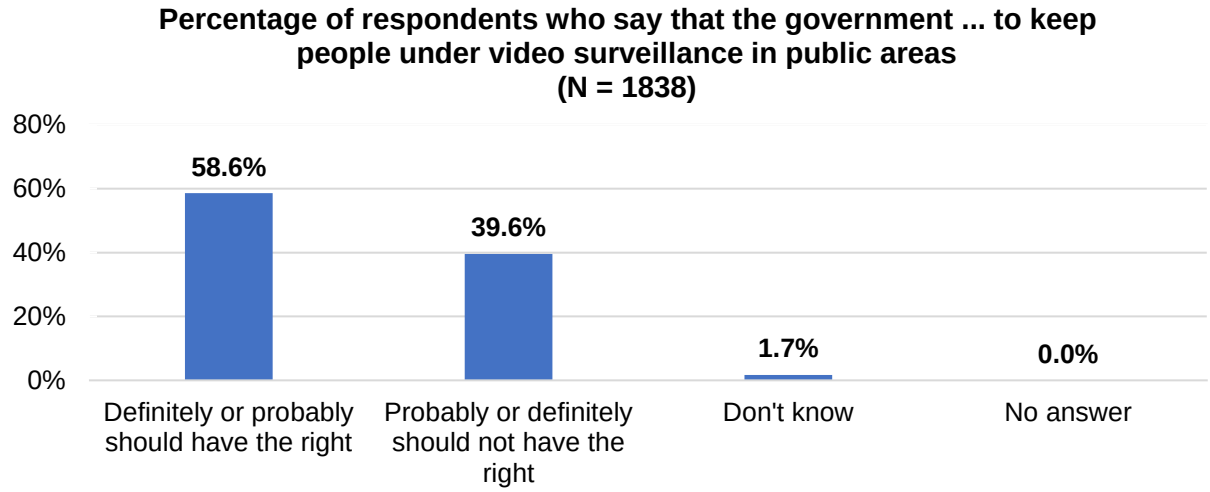

Fig. 2. Respondents' attitudes towards video surveillance by their government (cf. EVS/WVS 2021c, p. 428).

In contrast, only a minority (27.1%) of Russian respondents agree that their government should be allowed to monitor emails and other information that is exchanged online (cf. EVS/WVS 2021c, p. 430) (Fig. 3).

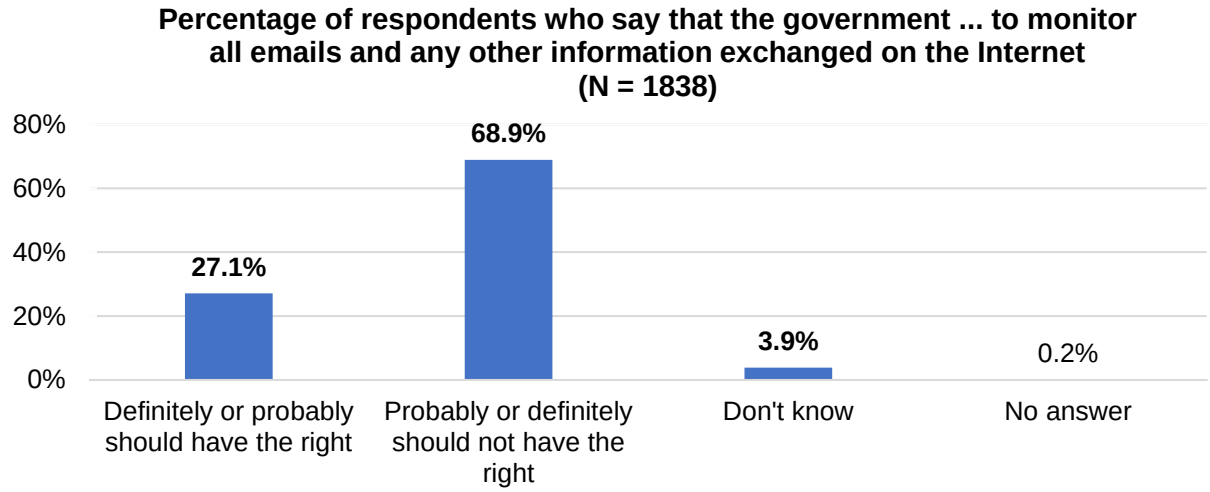

Fig. 3. Respondents' attitudes towards email and Internet monitoring by their government (cf. EVS/WVS 2021c, p. 430).

Russian respondents are also against (73.9%) their government having the right to collect data on anyone living in Russia without their knowledge (cf. EVS/WVS 2021c, p. 432) (Fig. 4).

[11] Here, the data of the EVS survey were used, as it included slightly more respondents than the WVS survey, which does, however, not differ significantly in the results.

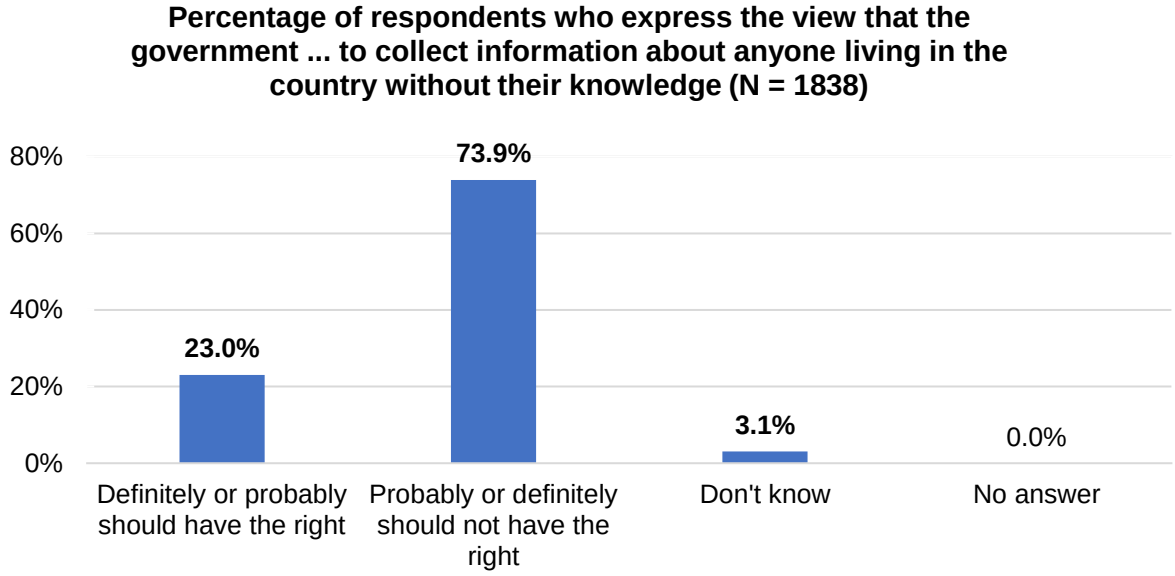

Fig. 4. Respondents' views on data tracking by the government without consent (cf. EVS/WVS 2021c, p. 432).

No recent large-scale survey on Russians' attitudes towards surveillance at the workplace could be found. Neither PwC (2021) nor Unisys (2021), which contain relevant data for other countries, provide data on this topic for Russia.

With regard to the use of collected personal data by companies, 52% of Russian respondents somewhat or strongly agree that consumers should be able to refuse this. Furthermore, 46% believe that consumers should be paid or rewarded if they allow companies to use their data. Only a minority of 19% of Russian respondents do not mind if companies use collected data (cf. Ipsos 2019, p. 12) (Fig. 5).

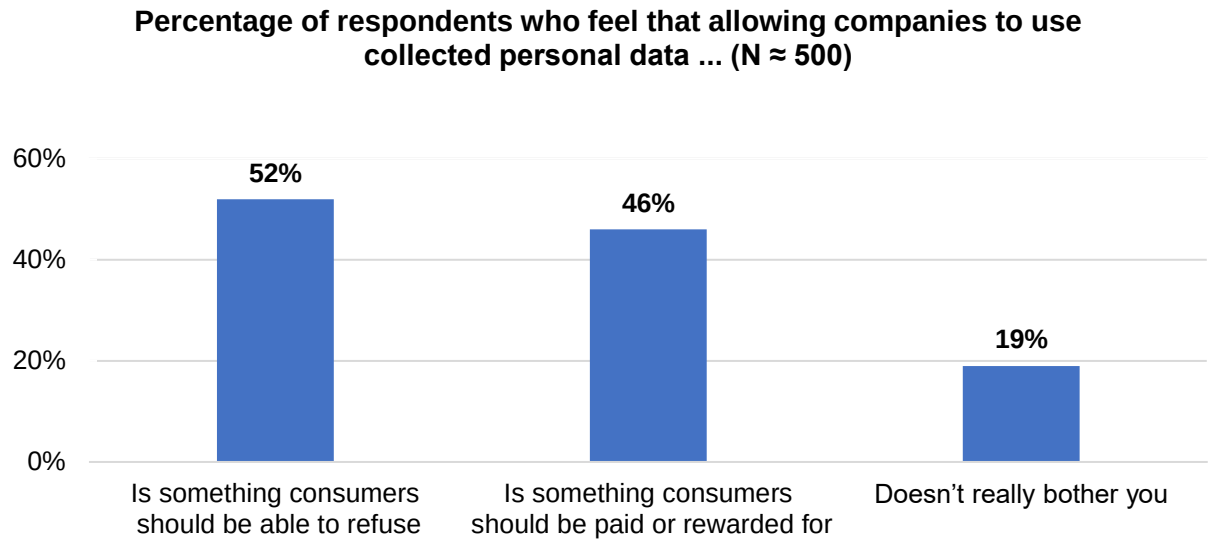

Fig. 5. Attitudes towards being able to refuse the use of collected data by companies or being paid/rewarded (cf. Ipsos 2019, p. 12).

V. Degree of Privacy of Data

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

For an indication of what types of personal data are considered particularly private or sensitive in Russia, let us take a look at their legal definition. Data protection rules can be "found in specific legislation, particularly the Data Protection Act No. 152 FZ dated 27 July 2006 (DPA)" (DLA Piper 2021a). First of all, personal data are defined there as "any information referring directly or indirectly to a particular or identified individual (hereinafter referred to as 'personal data subject'" (DPA[13] Chapter 1, Article 3; cf. also DLA Piper 2021). Sensitive personal data "include data related to race, national identity, political opinions, religious and philosophical beliefs, health state, intimacies and biometrical data" (DLA Piper 2021b). In addition, Chapter 2, Article 10 of the DPA categorizes personal data concerning ethnic origin and sexual life as "[s]pecial".

No recent large-scale survey on Russians' opinions on what constitutes sensitive data could be found. Neither Trepte and Masur (2016), Fukuta et al. (2017), nor Markos, Milne, and Peltier (2017), which contain relevant data for other countries, provide data on this topic for Russia.

VI. Benefits Associated with Data Disclosure

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

A minority of Russian respondents (39%) believe that sharing personal data with companies makes it easier for them to offer customers better information, products, and services for their individual needs. Almost the same percentage of respondents (38%) think that it makes it easier for them as consumers to find relevant information, products, and services. 33% indicate that the disclosure of personal data to companies can help them (as consumers) save time and 18% agree that it can help them save money (cf. Ipsos 2019, p. 12) (Fig. 6).

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

[13] https://pd.rkn.gov.ru/authority/p146/p164/?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (last access: 03/01/2022).

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

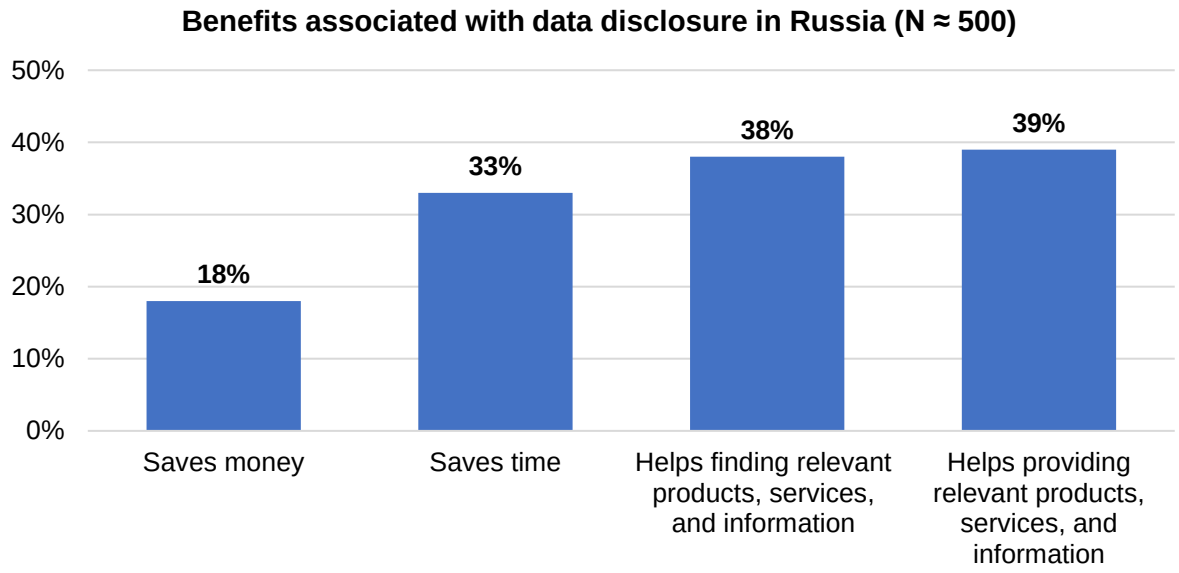

Fig. 6. Benefits associated with data disclosure in Russia (cf. Ipsos 2019, p. 12).

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), only 29% of Russian respondents indicate six- or seven-point agreement (cf. GfK 2017, p. 35).

VII. Privacy Concerns and Risks

[This] parameter […] comprises the negative effects [Russian 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

People are less willing to disclose data to companies when data breaches occur. A majority of 71% of Russian respondents feel more comfortable disclosing their data to companies that have "never been subject to any breach, leak, or fraudulent usage of data" (cf. Ipsos 2019, p. 14).

Moreover, 88% of Russian respondents want their "online data & personal information" to be "stored on a secure server", preferably "in their own economy" (as indicated by 79%) (CIGI-Ipsos 2019b, pp. 13, 15). 41% want their data to be stored abroad and 37% do not care if their data leave Russia (cf. CIGI-Ipsos 2019b, pp. 17, 19) (Fig. 7).

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

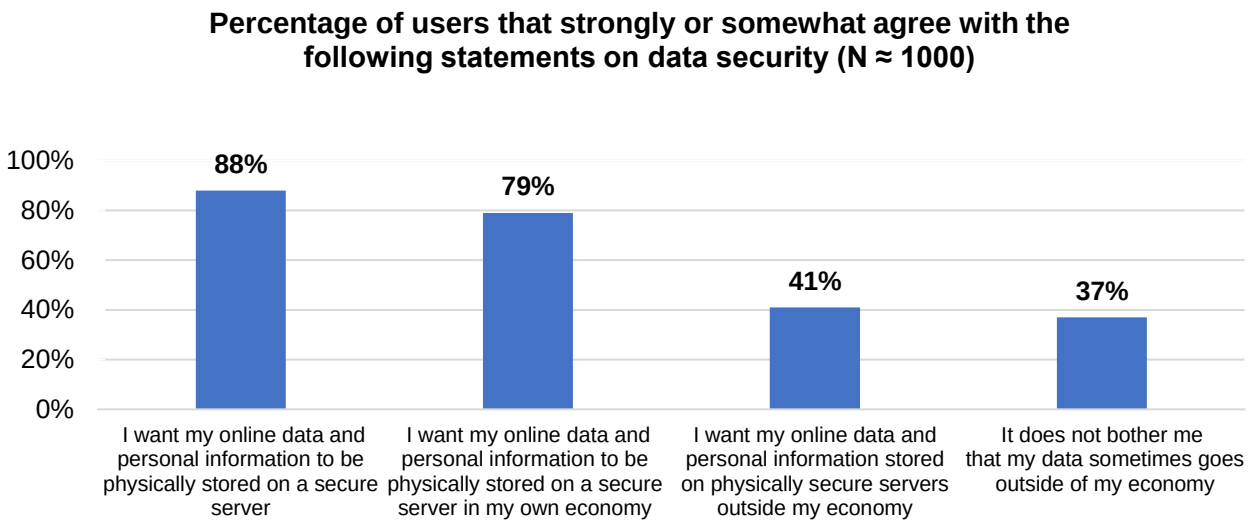

Fig. 7. Percentage of users that strongly or somewhat agree with the respective statements on data security (cf. CIGI-Ipsos, 2019b, pp. 13, 15, 17, 19, CIGI-Ipsos, 2019c, p. 283).

2. Concerns and Risks related to Data Control

About half of the respondents from Russia report that they use the Internet more selectively (51%) and a majority says that they disclose fewer personal data online (62%) because they do not trust the Internet. 39% put more effort into securing their devices, 22% self-censor what they say online, and 21% report they make fewer online purchases as a consequence of their distrust of the Internet (cf. CIGI-Ipsos 2019c, p. 24) (Fig. 8).

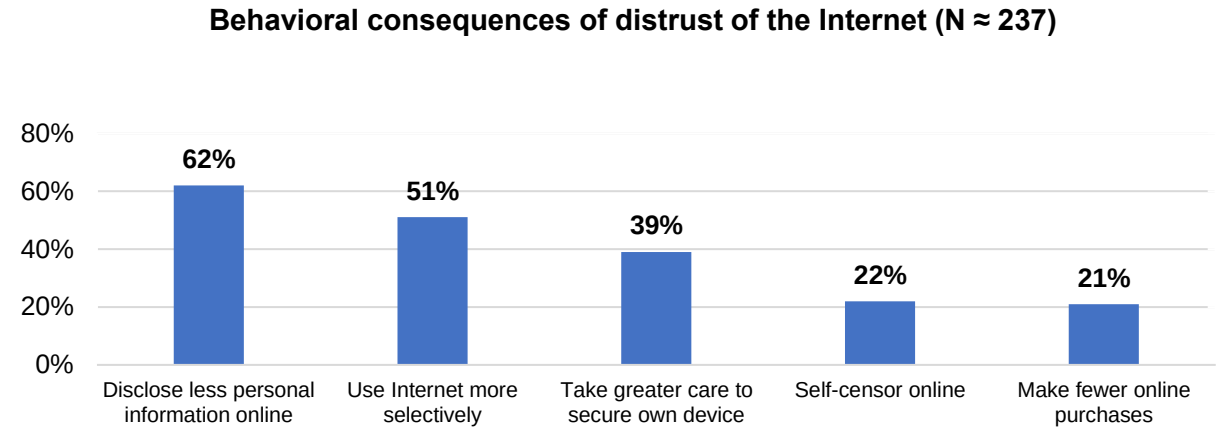

Fig. 8. Behavioral consequences of distrust of the Internet (cf. CIGI-Ipsos 2019c, p. 24).

VIII. Data Protection Literacy

[Data Protection Literacy] captures [Russian 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]

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

Half of the Russian respondents (50%) are very or somewhat aware of the data protection and privacy rules of their country (cf. CIGI-Ipsos 2019b, p. 8, 2019c, p. 281) (Fig. 9).

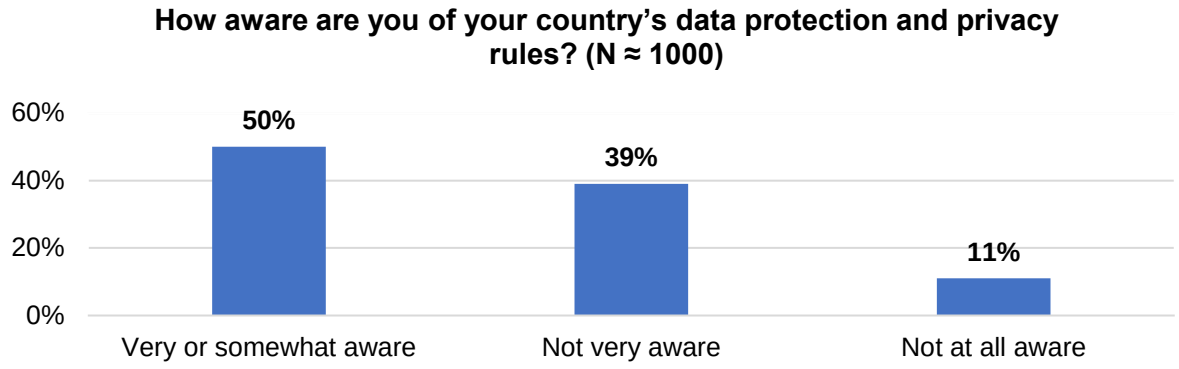

Fig. 9. Awareness of data protection and privacy rules in Russia (cf. CIGI-Ipsos 2019c, p. 281).

Nevertheless, a clear majority of 69% of Russian respondents feel that they do enough to protect their own data (16% strongly and 53% somewhat agree) (cf. CIGI-Ipsos 2019b, p. 29, 2019c, p. 283).

No recent large-scale survey of Russians' evaluation of their data protection law could be found. Cisco (2021), which contains relevant data for other countries, does not provide data on this topic for Russia.

IX. Attitudes Towards Data Receiver

[This] parameter […] refers to [Russian 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 low among Russian respondents. A large majority (73.9%) feels that most people cannot be trusted (cf. EVS/WVS 2021a, p. 7, 2021c, p. 175)[18] (Fig. 10).

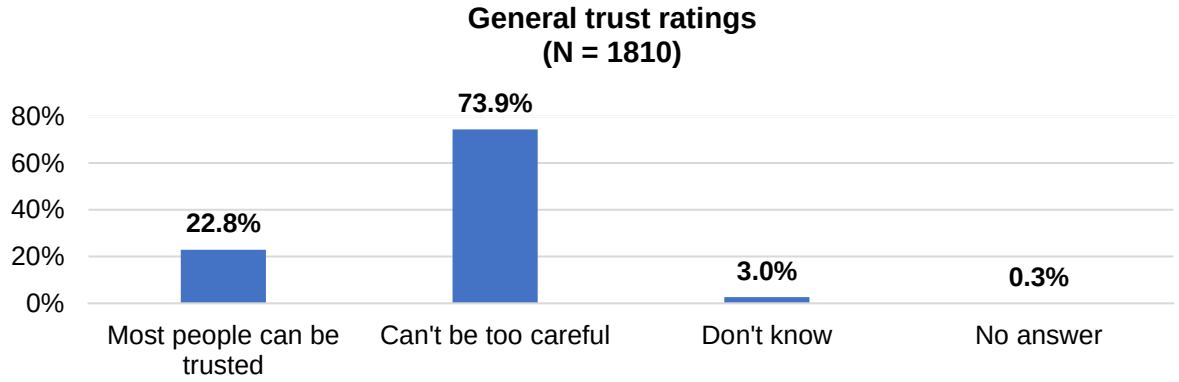

Fig. 10. Trust towards others in Russia (cf. EVS/WVS 2021c, p. 175).

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

[18] Here, the data of the EVS survey were used, as it included slightly more respondents than the WVS survey, which does, however, not differ significantly in the result.

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

1. Attitudes Towards Governments

Russians' attitudes towards political institutions except their government reflect the prevailing general distrust towards others. Majorities of the respondents report that they do not really trust political parties (61.6%) and parliament (51.8%). However, more than half of the respondents from Russia (53%) indicate that they trust their government "a great deal" or "quite a lot" (EVS/WVS 2021c, pp. 266, 273, 275) (Fig. 11).

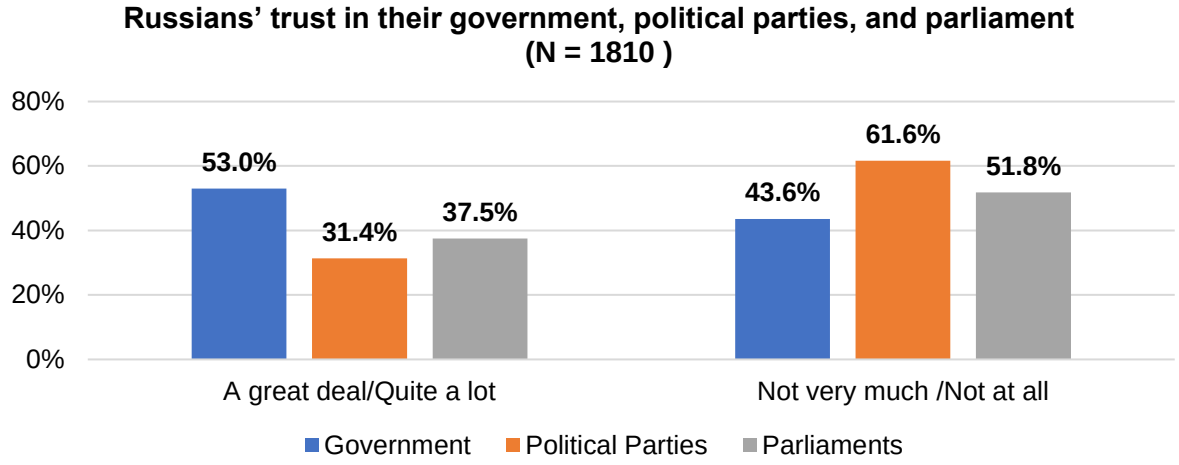

Fig. 11. Russians' trust in their government, political parties, and parliament (cf. EVS/WVS 2021c, pp. 266, 273, 275).

However, less than half of the respondents from Russia (44%) agree (somewhat or strongly) that their government's efforts to protect their data are sufficient (cf. CIGI-Ipsos 2019b, p. 45).

Russians' confidence that their government uses their personal data correctly is not very strong. Only 36% trust their domestic government in this respect and even less, 14%, have confidence in foreign governments (cf. Ipsos 2019, p. 20) (Fig. 12).

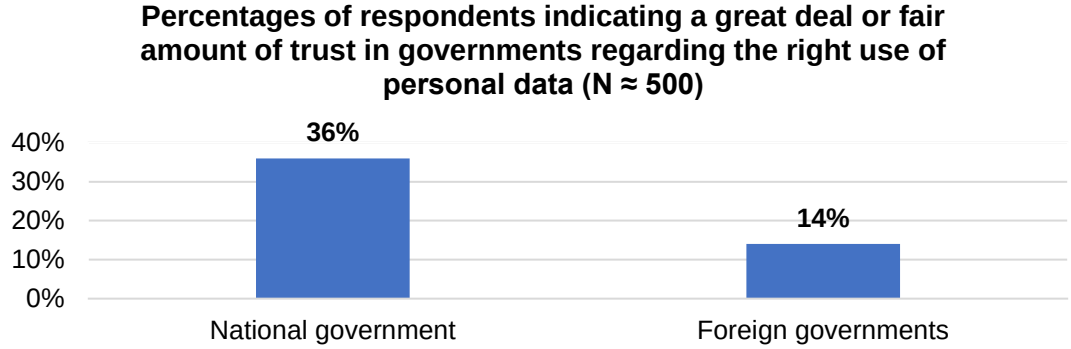

Fig. 12. Percentages of respondents indicating a great deal or fair amount of trust in governments regarding the right use of personal data (cf. Ipsos 2019, p. 20).

Besides, more than two-thirds of Russian respondents (69%) report that their national government contributes to their distrust of the Internet, and 66% indicate this with regard to foreign governments (cf. CIGI-Ipsos 2019a, p. 117, 119, 2019c, p. 20) (Fig. 13).

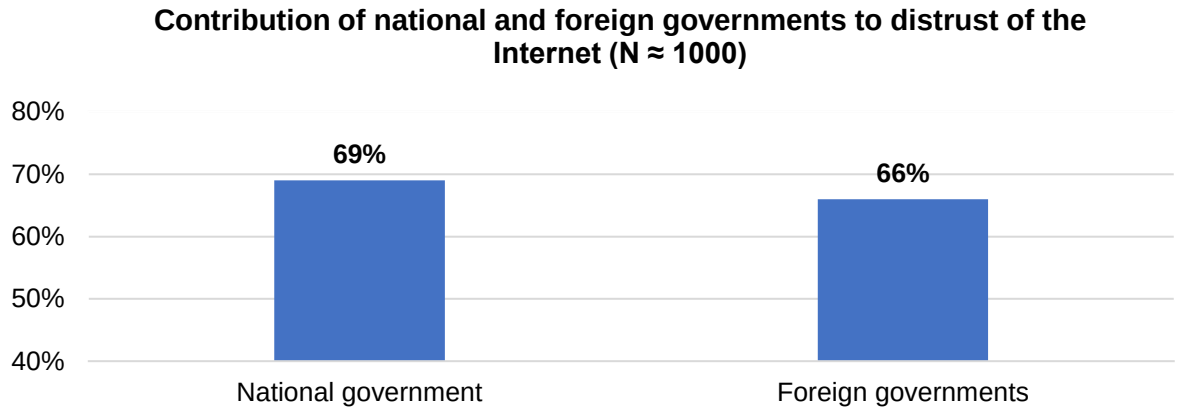

Fig. 13. Contribution of national and foreign governments to distrust of the Internet (cf. CIGI-Ipsos 2019a, pp. 117, 119, 2019c, p. 20).

2. Attitudes Towards Companies

Russians trust companies more than their government with their data: 60% of respondents think that companies do enough to protect their data but only 44% agree that their government's efforts are sufficient in this respect (cf. CIGI-Ipsos 2019c, p. 283) (Fig. 14).

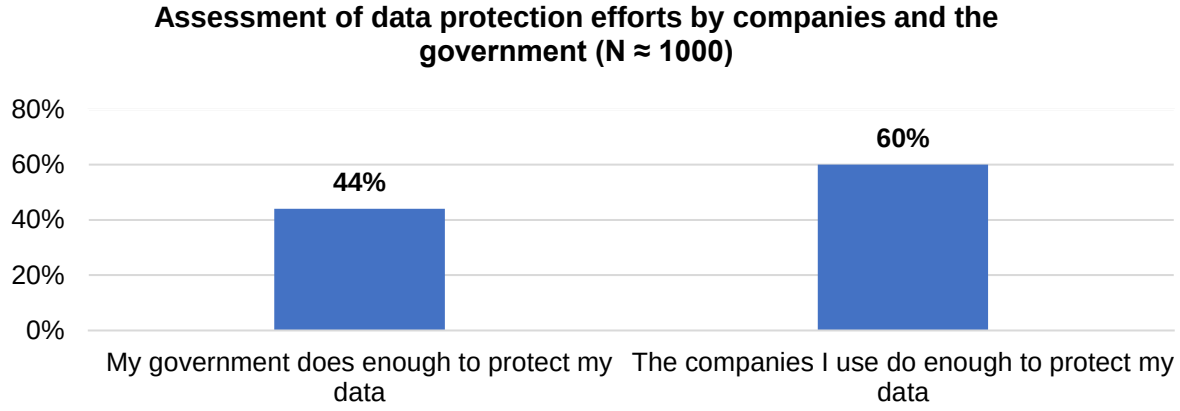

Fig. 14. Percentage of respondents that strongly or somewhat agree that companies' and their government's efforts suffice to protect their data (cf. CIGI-Ipsos 2019c, p. 283).

Russians' confidence in companies to use their data correctly varies when looking at different industries. The only sector in which a majority (53%) trusts is healthcare providers, all other sectors are trusted by less than half of the respondents to handle their data properly: financial services companies (43%), telecommunications companies (33%), shipping and delivery companies (32%), search and social media sites (21%), retailers (20%), and media companies (18%) (cf. Ipsos 2019, p. 20) (Fig. 15).

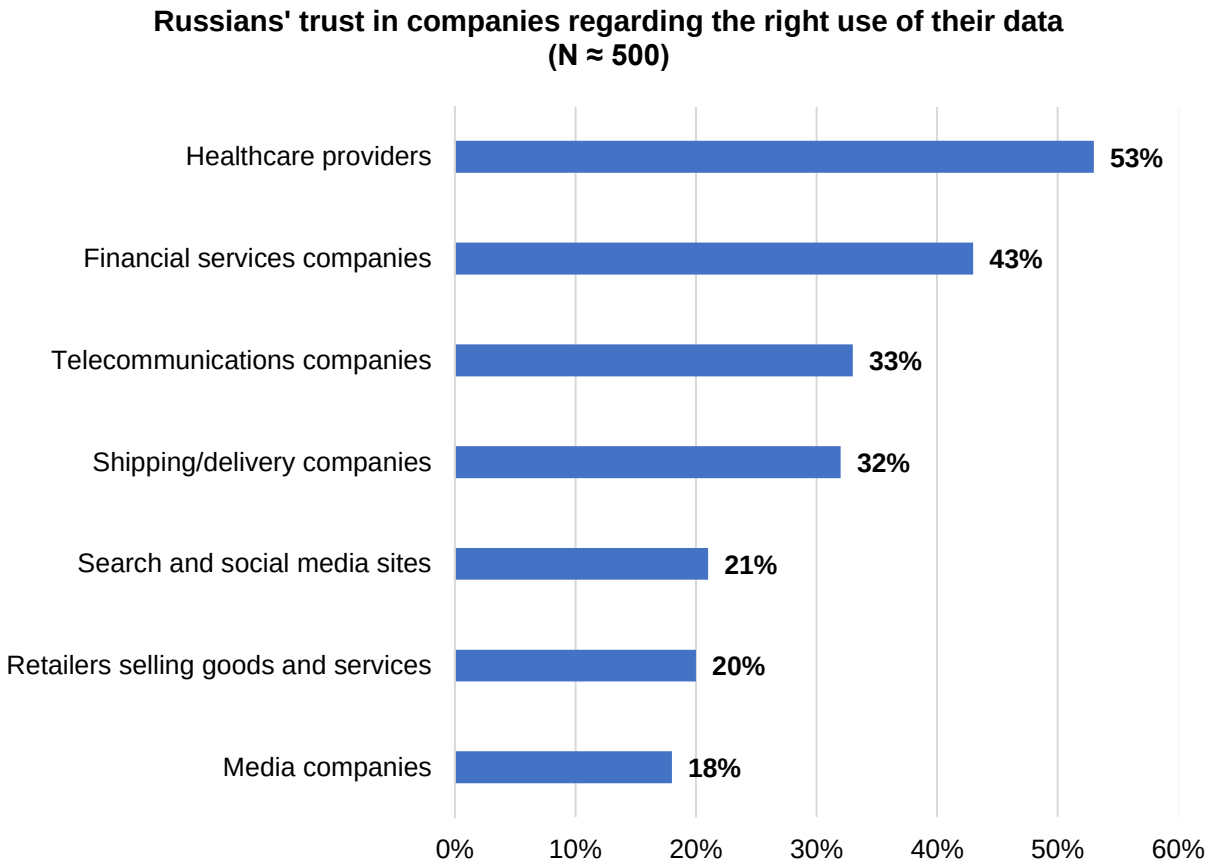

Fig. 15. Russians' trust in companies regarding the right use of their data (cf. Ipsos 2019, p. 20).

Besides, the following institutions are reported to contribute to distrust of the Internet by respondents from Russia: social media companies (76%), e-commerce platforms, online and mobile banking platforms (both 61%), Internet service providers, and search engines (both 59%) (cf. CIGI-Ipsos 2019c, p. 20) (Fig. 16).

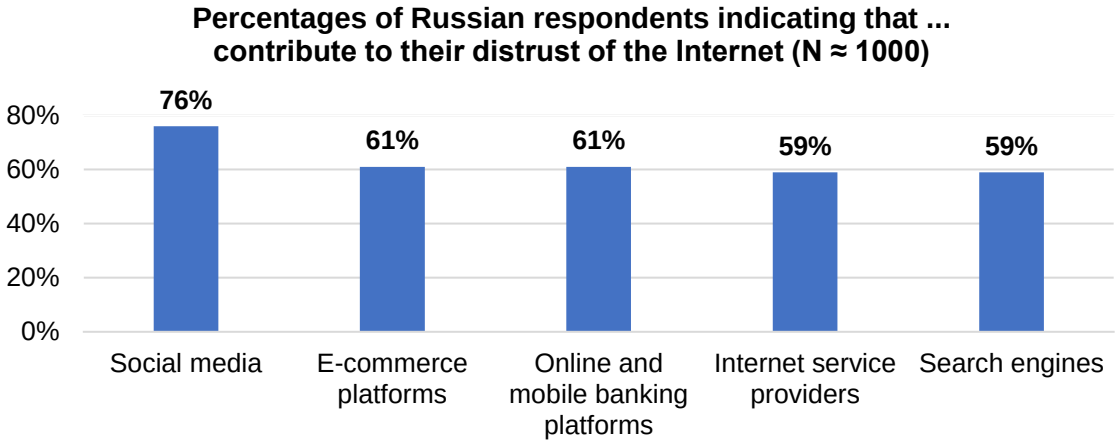

Fig. 16. Percentages of Russian respondents feeling that the mentioned institutions contribute to their distrust of the Internet (cf. CIGI-Ipsos 2019c, p. 20).

X. Communication on Data Use

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

70% of Russian respondents would rather give their personal data to companies that communicate transparently what the data will be used for. 68% would feel better about disclosing their data to a company that committed explicitly to not passing them on to others (cf. Ipsos 2019, p. 14) (Fig. 17).

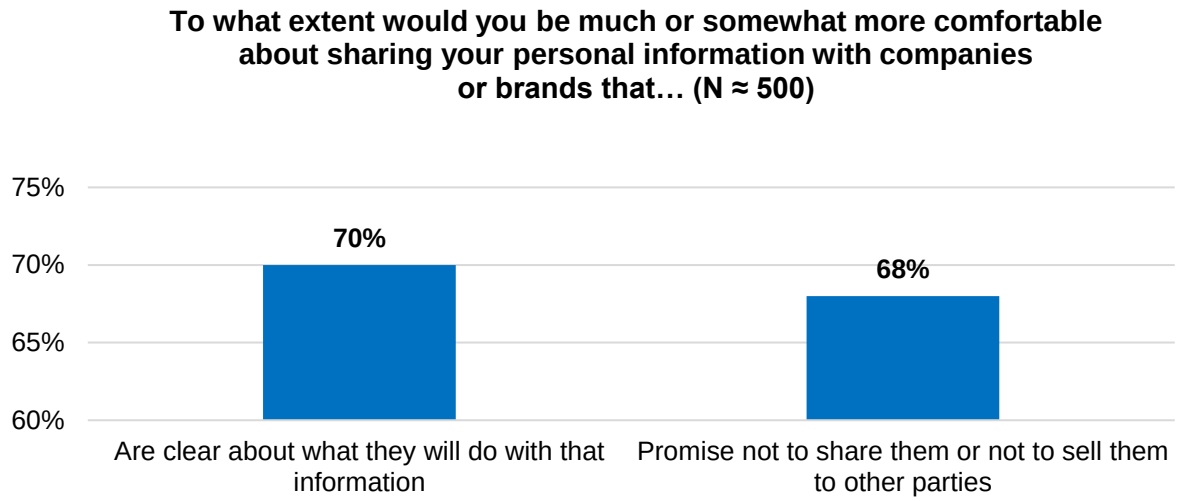

Fig. 17. Communication on data use (cf. Ipsos 2019, p. 14).

About half of the respondents from Russia (52%) report 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 Russians' WTS data (cf. Wawra 2022, IV. 3.).

1. Digital Competitiveness

For its overall performance, Russia is positioned 42nd out of 64 evaluated countries in the IMD (2021) ranking for digital competitiveness. It is thus among the last third of all countries.

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

Furthermore, it places among roughly the last quarter of all countries in two of the three main categories that indicate a country's digital competitiveness in the ranking: technology (rank 48) and future readiness for digitalization (rank 47). It is, however, among the best third (rank 24) in the category knowledge. Here it is even 6th in the subcategory training and education. Russia is one of the worst positioned countries for the subfactor capital in the category technology (rank 58), and for the subfactor business agility (rank 56) in the category future readiness. 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 general situational context and on the data receiver whether Russian respondents consider surveillance as more or less acceptable or not. A majority of Russian respondents (58.6%) accept governmental surveillance in public areas. However, only a minority approves of governmental email and Internet monitoring (27.1%) as well as secret data collection by the government in general (23%). Thus, informational privacy is attributed a significantly lower value in the context of state surveillance in the public sphere than in online environments, where it is of high importance for the vast majority of Russian respondents. Moreover, informational privacy is highly valued when it comes to surreptitious state intervention. No recent large-scale survey on Russians' attitudes towards surveillance at the workplace could be found. Neither PwC (2021) nor Unisys (2021), which contain relevant data for other countries, provide data on this topic for Russia. This survey gap should be closed by future studies.

Regarding the use of collected personal data by companies, more than half of the respondents (52%) from Russia agree that consumers should have the right to refuse this. For a small majority, it is thus important to preserve their informational privacy when dealing with companies. Only about a fifth of the Russian respondents (19%) do not mind if companies use collected personal data. A minority, 46%, of Russian respondents believe that consumers should be compensated for the use of their data. So, a majority does not generally put a 'price tag' on their informational privacy.

3. Degree of Privacy of Data

In Russia, sensitive personal data are usually referred to as sensitive personal information in legal texts. Sensitive personal information can be directly or indirectly linked to an individual or 'data subject' (in the diction of the legal text) if it is disclosed. It includes data related to

- race and ethnicity
- national identity
- political opinions
- religious and philosophical beliefs
- health state and sexual life/ intimacies and
- biometrical data

No recent large-scale survey on Russians' opinions on what constitutes sensitive data could be found. Neither Trepte and Masur (2016), Fukuta et al. (2017), nor Markos, Milne, and Peltier (2017), which contain relevant data for other countries, provide data on this topic for Russia. This

is a research gap that should be addressed by future studies, especially as the perceived degree of privacy or sensitivity of data has been identified as a factor that seems to have one of the greatest impacts on people's WTS personal data (cf. Wawra 2022). Ackermann et al. (2021) for example state:

"The more sensitive a particular type of data is perceived, the less impact do other factors have on corresponding WTS-decisions. 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."

4. Benefits Associated with Data Disclosure

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

- companies to better tailor information, products, and services to their needs (39%)
- them as consumers to find relevant information, products, and services (38%)
- them as consumers save time (33%) and money (18%).

Thus, majorities do not consider any of these as benefits of data disclosure. This is certainly one explanation why, when asked directly about their willingness to disclose, less than a third of Russian respondents (29%) say they would be very willing to share personal data (6- or 7-point agreement on a 7-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). Besides, health and financial data as well as driving records and information on energy use were mentioned as examples of personal data in the survey. However, the survey did not differentiate between these different types of data either. As health data are sensitive personal data according to Russian law (see Degree of Privacy of Data above), and as these and financial data have often been categorized by a majority as sensitive or being above a medium privacy threshold in other cultures (cf. e.g. Trepte and Masur 2016, Fukuta et al. 2017, Roose, Pang 2021), this could also explain why a majority of Russian 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) (see above) conclude that the higher the perceived sensitivity of data, the less other variables (such as benefits of disclosure) affect people's WTS data. If, however, data are "not perceived as very sensitive, other factors, such as what compensation is offered […], 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 Russian data disclosure culture. Furthermore, they should systematically differentiate between different kinds of benefits as there might be cultural differences with regard to which value is attributed to different kinds of 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

Data Security is important to Russians: A clear majority of respondents (71%) would be more comfortable sharing personal information with a company that has never experienced a breach, leak, or fraudulent usage of data. Moreover, a majority of 88% wants their data to be stored on a secure server, preferably in their own country (79%). A minority, 41%, wants their data to be stored abroad, and a bit more than a third (37%) of the respondents from Russia do not mind if their data leave the country. Consequently, an impeccable track record of data security and data storage in the country should have a positive impact on the willingness of most Russians to share personal data.

b. Data Control

Because of their concerns about control over their data on the Internet, a majority of respondents from Russia report that they disclose less personal information online (62%), about half use the Internet more selectively (51%). 39% indicate that they take greater care to secure their devices, and 22% self-censor what they say online. About one-fifth (21%) says they make fewer purchases online.

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 Russian respondents.

6. Data Protection Literacy

Half of the respondents from Russia (50%) are aware of the data protection and privacy rules that apply in their country. More than two-thirds (69%) report that their efforts to protect their own data are sufficient. No recent large-scale survey of Russians' evaluation of their data protection law could be found. Cisco (2021), which contains relevant data for other countries, does not provide data on this topic for Russia. This is another research gap that should be closed by future studies. Furthermore, 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, Russians' trust in others is low with only 22.8% saying that most people can be trusted and 73.9% expressing caution in this respect. Russians' trust in political institutions except their government follows this trend: A majority (61.6%) reports that they do not trust political parties very much or not at all, and 51.8% say this for parliament. In contrast, a majority (53%) indicates that they trust their government a great deal or quite a lot. However, fewer than half of the respondents (44%) agree that their government's efforts to protect their data are sufficient. Even less, a bit more than a third (36%) has confidence in their government that they use personal data

correctly, and 14% trust foreign governments in this respect. In addition, a majority indicates that their national government (69%) and foreign governments (66%) add to their lack of confidence in the Internet. All in all, it is therefore to be expected that the basic WTS data with their own and foreign governments is not great among a majority of Russians.

b. Attitudes Towards Companies

A majority of Russians (60%) consider the data protection measures of the companies they have done business with to be sufficient. Russians' trust in companies with regard to the proper use of their data varies, depending on the respective industry. More than half of the respondents only trust healthcare providers (53%) in this respect, followed by financial services companies (43%), telecommunications companies (33%), shipping/delivery companies (32%), search and social media sites (21%), retailers (20%), and media companies (18%), i.e. distrust prevails with regard to most industries when it comes to the correct use of personal data. Moreover, the following institutions contribute to Russians' distrust of the Internet (besides governments, see above): social media companies (76%), e-commerce platforms, online and mobile banking platforms (both 61%), Internet service providers, and search engines (both 59%). From this, we can deduce the general tendency that for the majority of Russians, the WTS data is highest towards healthcare providers.

8. Communication on Data Use

A majority of Russian respondents would be more willing to disclose personal data if companies communicated the use of the data transparently (70%) and promised that they would not pass on the data (68%). About half of the respondents (52%) indicate that it would also help if potential risks were communicated clearly. So, if companies convey these contents, this should potentially have a positive impact on the WTS data of a majority of people from Russia.

XII. Conclusion and Outlook

This study captures the narrower cultural context of data disclosure in Russia (cf. Wawra 2022, II. 8., III.). It provides an overview of Russian 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 Russia by shedding light on the prevailing attitudes, assumptions, views, and reported behaviors of respondents from Russia that can influence their WTS personal data.

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

- the value Russian respondents place on their informational privacy in different contexts
- which kinds of data are defined as sensitive personal data according to Russian law
- 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 Russians place on data security
- reported behavior that follows from perceived privacy concerns and risks

- Russians' awareness of data protection and privacy rules and the evaluation of their own data protection efforts
- Russians' general trust levels and their trust in domestic and foreign governments and different types of companies, as well as their trust in these institutions with regard to their personal data
- 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 Russian 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).

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: 01/20/2022).

DLA Piper (2021a). Data Protection Laws of the World: Russia – Law. https://www.dlapiperdataprotection.com/index.html?t=law&c=RU (last access: 01/18/2022).

DLA Piper (2021b). Data Protection Laws of the World: Russia – Definitions. https://www.dlapiperdataprotection.com/index.html?t=definitions&c=RU&c2= (last access: 01/18/2022).

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).

Fukuta, Y., Murata, K., Adams, A. and Orito, Y. (2017). Personal Data Sensitivity in Japan: An Exploratory Study. ORBIT Journal 1(2). DOI: 10.29297/orbit.v1i2.40. https://www.researchgate.net/publication/317413763_Personal_Data_Sensitivity_in_Japan_An_Exploratory_Study (last access: 01/08/2022).

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).

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 Report 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).

Markos, E., Milne, G., Peltier, J. (2017). Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. https://doi.org/10.1509/jppm.15.159 (last access: 11/24/2021).

PwC (2021). Hopes and Fears 2021. https://www.pwc.com/gx/en/issues/upskilling/hopes-and-fears.html (last access: 01/08/2022).

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.

Roose, J., Pang, N. (2021). Data Security, Privacy and Innovation Capability in Asia: Findings From a Representative Survey in Japan, Singapore and Taiwan. Konrad Adenauer Stiftung (KAS). https://www.kas.de/documents/252038/11055681/Survey+on+Data+Security%2C+Privacy+and+Innovation+Capability+in+Asia.pdf/1b96fbea-5f0c-5716-dbc4-a426eca190bc?version=1.0&t=1628241322758 (last access: 01/07/2022).

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).

Unisys (2021). 2021 Unisys Security Index™: Global Report. https://www.unisys.com/siteassets/microsites/unisys-security-index-2021/report-usi-2021.pdf (last access: 11/15/2021).

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[20]

Study	Overview	Sample size	Demographics
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 ≈[21] 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	Age of respondents: 16 - 64 Online population
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 = 1501	"The data have been weighted to reflect the demographic composition of the online population age 15+" (GfK 2017, p. 4).

[20] 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 Russia.

[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
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 Russia 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).

[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).