IRDG Institut für das Recht der digitalen Gesellschaft

UNIVERSITY OF PASSAU Faculty of Law

UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES NO. 22-10

CULTURAL INFLUENCES ON PERSONAL DATA DISCLOSURE DECISIONS

Japanese 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 Japan on central parameters that can influence people's willingness to share (WTS) personal data. It provides insights into Japanese 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 – Japanese Perspectives. *University of Passau Institute for Law of the Digital Society Research Paper Series No. 22-10.* https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/.

Keywords

Culture, Data Disclosure, Digitalization, Information Governance, Privacy, Japan, 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 Japanese 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 Japan. 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).

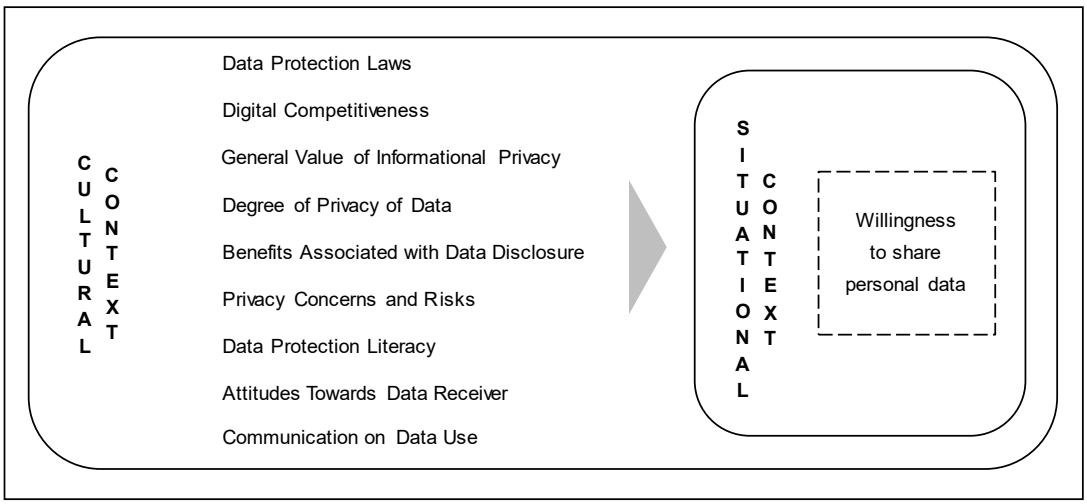

Fig. 1. Central parameters of data disclosure (from Wawra 2022).

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 Japan. The sample size was usually 1000 or more, one study included about 200 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, Japan is ranked 28th out of 64 countries in 2021 for digital competitiveness. It receives the 25th rank for its advances in **knowledge**, rank 30 in the category **technology**, and 27 in **future readiness** for digitalization. When looking at the five- year development, Japan's rankings have slightly worsened, with the exception of the category knowledge: Its overall (from 27th in 2017 to 28th in 2021) and future readiness rankings (from 25th in 2017 to 27th in 2021) have only declined marginally. Its placement in the category technology has deteriorated a little more (from 23rd in 2017 to 30th in 2021). Its ranking for knowledge, however, has somewhat improved (from 29th in 2017 to 25th in 2021) (cf. IMD 2021, p.104).

Subfactor rankings with regard to **knowledge** position Japan 47th in the subcategory **talent** and 62nd for personnel's digital and technological skills, which is one of the items of this category. Japan is 21st in the subcategory **training and education** and 13th in **scientific concentration**[6] (cf. IMD 2021, p.105).

In the field of **technology**, Japan ranks 48th in the subcategory of **regulatory framework** and 44th for starting a business as well as 49th for development & application of technology, two of the items in this subcategory. For the subfactor **capital**, Japan occupies 37th place and ranks 36th for the funding for technological development. It ranks 8th for the subfactor **technological framework**[7], and here 37th for communications technology (cf. IMD 2021, p. 105).

In terms of **future readiness**, Japan ranks 18th for the subfactor **adaptive attitudes**, 53rd for **business agility**, and 23rd for **IT integration**. In the subcategory of adaptive attitudes, it ranks 4th for e-participation[8], and 21st for smartphone possession. In the subcategory of business agility, it occupies 63rd place with regard to the use of big data and analytics. In the final subcategory of IT integration, its ranks are 14th for e-government[9] and 44th for cyber security (cf. IMD 2021, p.105).

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 Japan 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 about Japanese people's assessment of the collection of personal data for surveillance by their government. A majority of Japanese respondents approve of

---

[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.).

governmental video surveillance in public: 57% agree that their government should have this right (cf. EVS/WVS 2021c, p. 427) (Fig. 2).

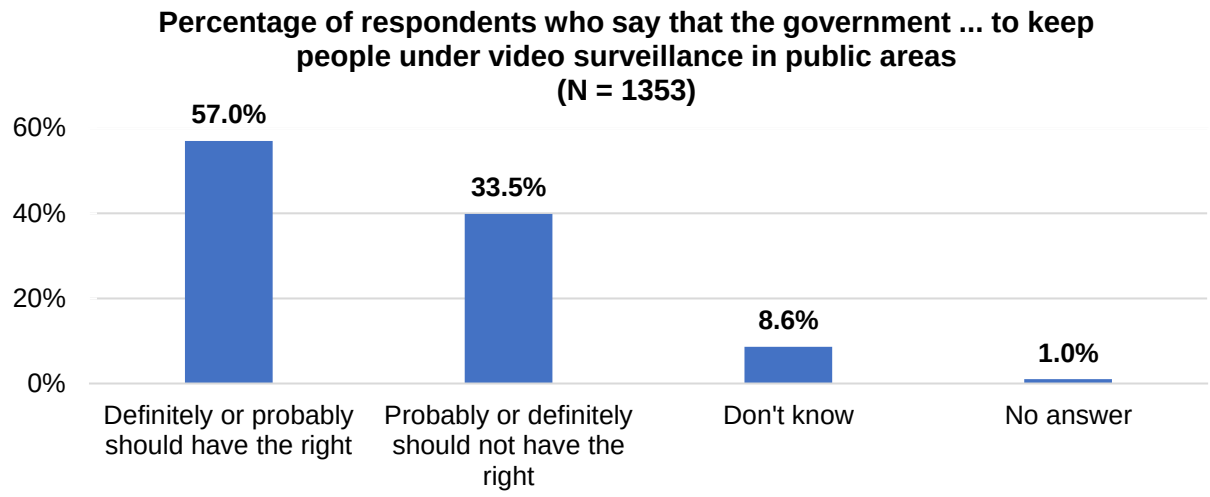

Fig. 2. Respondents' attitudes towards video surveillance by their government (cf. EVS/WVS 2021c, p. 427).

In contrast, only a minority (22.4%) of Japanese 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).

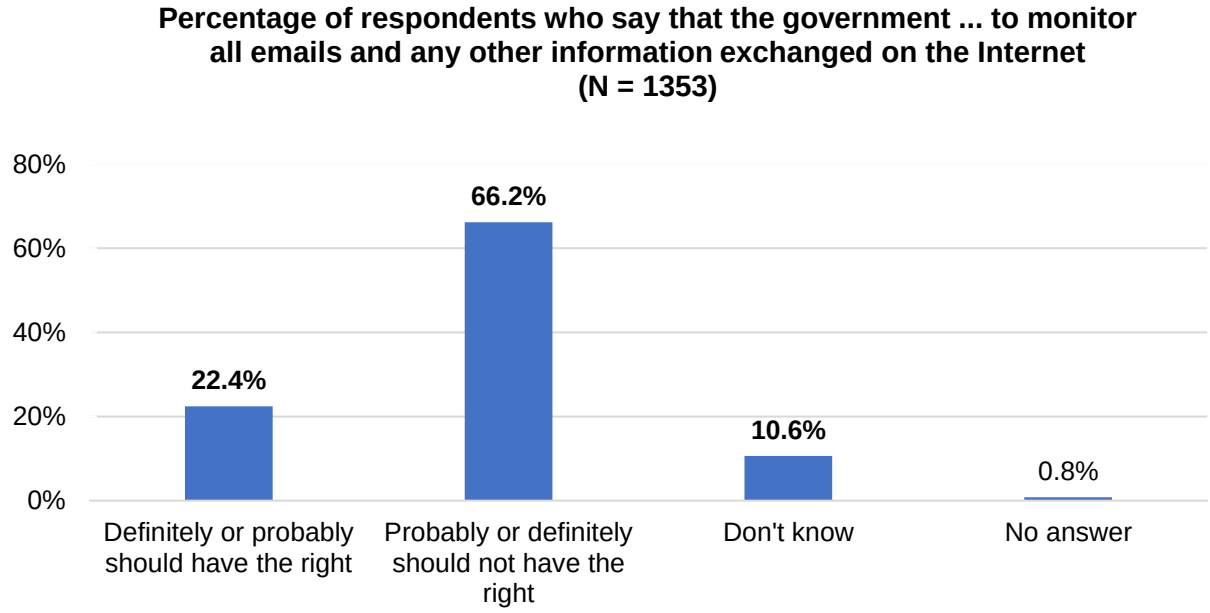

Fig. 3. Respondents' attitudes towards email and Internet monitoring by their government (cf. EVS/WVS 2021c, p. 429).

Even more Japanese respondents are opposed to data tracking by their government without their consent: 77.8% indicate that their government should probably or definitely not have the right to collect information about anyone living in the country without their knowledge (cf. EVS/WVS 2021c, p. 431) (Fig. 4).

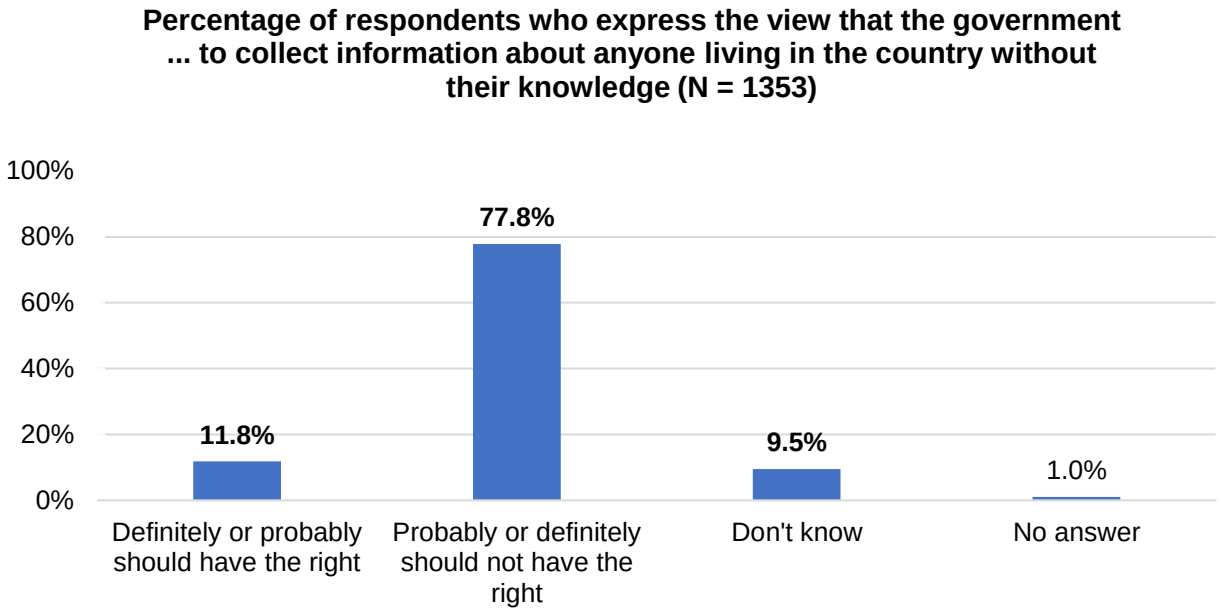

Fig. 4. Respondents' views on data tracking by the government without consent (cf. EVS/WVS 2021c, p. 431).

Surveillance at work is accepted by less than a quarter (22%)[11] of the respondents from Japan, who report that they do not mind if their employer uses technology, like sensors and wearable devices, to monitor their performance at work. An even smaller minority, 16%[12], is not opposed to their employer having access to their personal data like their social media profile (cf. PwC 2021, p. 17).

With regard to the use of collected personal data by companies, 51% of Japanese respondents somewhat or strongly agree that consumers should be able to refuse this. Furthermore, 41% believe that consumers should be paid or rewarded if they allow companies to use their data. Only a minority of 11% of Japanese respondents do not mind if companies use collected data (cf. Ipsos 2019, p. 12) (Fig. 5).

[11] This percentage is rounded as the Japanese report does not provide an aggregated percentage but separate percentages for full time (ft), part time (pt) and contract workers (cw). The average of the three percentages that indicate the approval rates of Japanese respondents, 29% (ft), 22% (pt), and 16% (cw), is 22.33%.

[12] This percentage is rounded as the Japanese report does not provide an aggregated percentage but separate percentages for full time (ft), part time (pt) and contract workers (cw). The average of the three percentages that indicate the approval rates of Japanese respondents, 20% (ft), 15% (pt), and 12% (cw), is 15.66%.

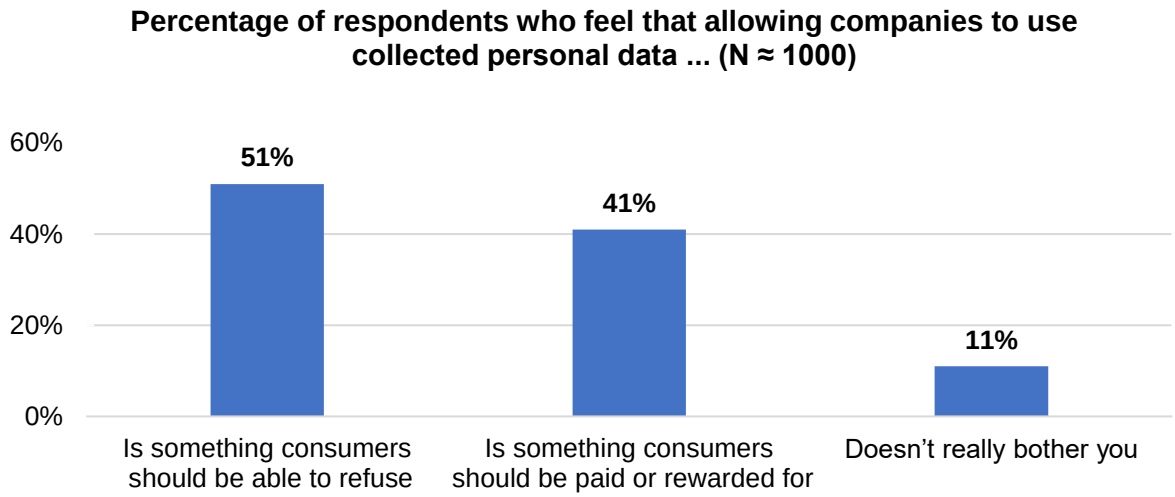

Fig. 5. Attitudes towards being able to refuse the use of collected data by companies or being paid/rewarded (cf. Ipsos 2019, p. 12).

V. Degree of Privacy of Data

[This] parameter […] surveys how private or sensitive […] certain kinds of personal data [are for Japanese respondents].[13]

An indication of what types of personal data are considered particularly private in Japan is provided by the Act on the Protection of Personal Information (APPI). According to this law,

"[p]ersonal information is information about a living individual which can identify a specific individual by name, date of birth or other description contained in such information. Personal Information includes information which enables one to identify a specific individual with easy reference to other information" (DLA Piper 2021).

Sensitive information

"includes information about a person's race, creed, social status, medical history, criminal record, any crimes a person has been a victim of, and any other information that might cause the person to be discriminated against"[14] (DLA Piper 2021).

Asked about their willingness to disclose specific kinds of personal data online for better services, a majority of Japanese respondents answered in each case that they would be very or somewhat unwilling to share the following data, which can thus be categorized as sensitive: their "bank account balance" (65%), "demographic data (e. g. your name, your address)" (55%) and their "medical records (e. g. X-rays, CT scans)" (52%) (Roose, Pang 2021, p. 37). In another study by Fukuta et al. (2017), ID numbers[15] turned out to be the most sensitive data for Japanese respondents (with a mean of M = 2.460 on a four-point Likert scale), followed by financial information[16] (M = 2.423). Further categories of sensitive data that were above a medium privacy threshold (of M = 2) were

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

[14] cf. also Amended Act on the Protection of Personal Information 2020, Chapter I, Article 2(3), https://www.ppc.go.jp/files/pdf/APPI_english.pdf (last access: 03/07/2022).

[15] This category contained e.g. pension/social security number, health insurance, taxpayer, and driving license number.

[16] e.g. personal income, tax paid and real estate ownership.

information on crimes[17], sensitive biometrics[18] (both M ≈ 2.3), the digital persona[19] (M ≈ 2.2), health and well-being[20] (M ≈ 2.15), contact numbers[21] (M ≈ 2.1), social categories[22], and social relationships[23] (both M ≈ 2.0) (in this order, according to mean values, which were not further specified in the study when reported here with ≈ according to figure 1 of the study). Further types of personal data that were surveyed in the study and turned out to be below a medium privacy threshold (M < 2.0), were, in declining order, civics[24] (1.787), data shadow[25] (1.773), non-sensitive biometrics[26] (M ≈ (almost) 1.5), and personal ID[27] (M ≈ 1.45) (cf. Fukuta et al. 2017).

VI. Benefits Associated with Data Disclosure

[This] parameter […] renders the positive effects [Japanese respondents] expect from the disclosure of their personal data.[28]

Less than half of the Japanese respondents (27%) 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 participants in the survey (28%) think that it makes it easier for them as consumers to find relevant information, products, and services. 22% of the respondents 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).

[17] This category included criminal records, drug addiction, and records of having been the victim of a crime.

[18] This category contained e.g. data on fingerprints, iris scans, and DNA.

[19] This category included e.g. user ID, user name, and password.

[20] This category included e.g. data on diseases, degenerative conditions, and physical and mental disabilities.

[21] This category contained "home address, mobile/home phone number, and school/place of employment" (Fukuta et al. 2017).

[22] This category comprised "data in relation to family register, nationality and racial/ethnic background" (Fukuta et al. 2017).

[23] This category comprised "data representing networks or relationships in social life" (Fukuta et al. 2017).

[24] This category included data on political, religious, and sexual orientation.

[25] This category contained "records of web browsing, search keywords, library borrowing, and shopping" (Fukuta et al. 2017).

[26] This category included blood type, dental record, ear and foot shape.

[27] This category comprised data such as "name, day of birth, and place of birth" (Fukuta et al. 2017).

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

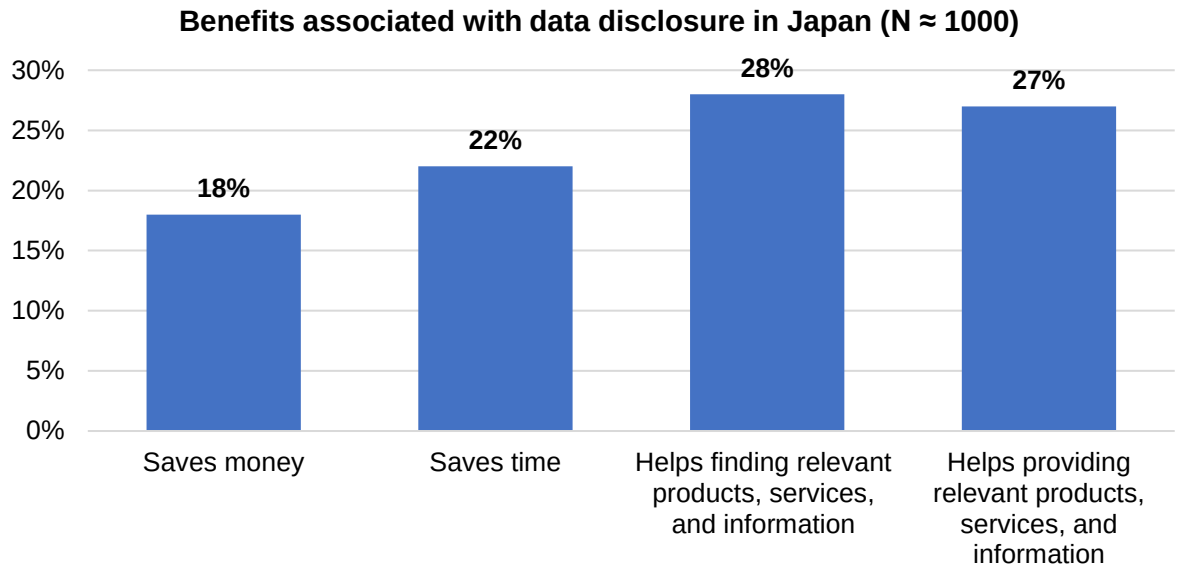

Fig. 6. Benefits associated with data disclosure in Japan (cf. Ipsos 2019, p. 12).

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 8% of Japanese respondents indicate six- or seven-point agreement (cf. GfK 2017, p. 78).

VII. Privacy Concerns and Risks

[This] parameter […] comprises the negative effects [Japanese respondents] associate with data disclosure. These include their general concerns about the security of their personal data, and their control over them.[29]

1. Concerns and Risks related to Data Security

A minority of respondents from Japan are less inclined to disclose data to companies that have experienced data breaches: 45% of Japanese respondents feel more comfortable disclosing their data to companies that have "never been subject to any breach, leak, or fraudulent usage of data" (Ipsos 2019, p. 14).

Moreover, 54% of Japanese respondents want their "online data & personal information" to be "stored on a secure server", preferably "in their own economy" (as indicated by 51%) (CIGI-Ipsos 2019b, pp. 13, 15). 37% want their data to be stored abroad and only 21% do not care if their data leave Japan (cf. CIGI-Ipsos 2019b, pp. 17, 19) (Fig. 7).

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

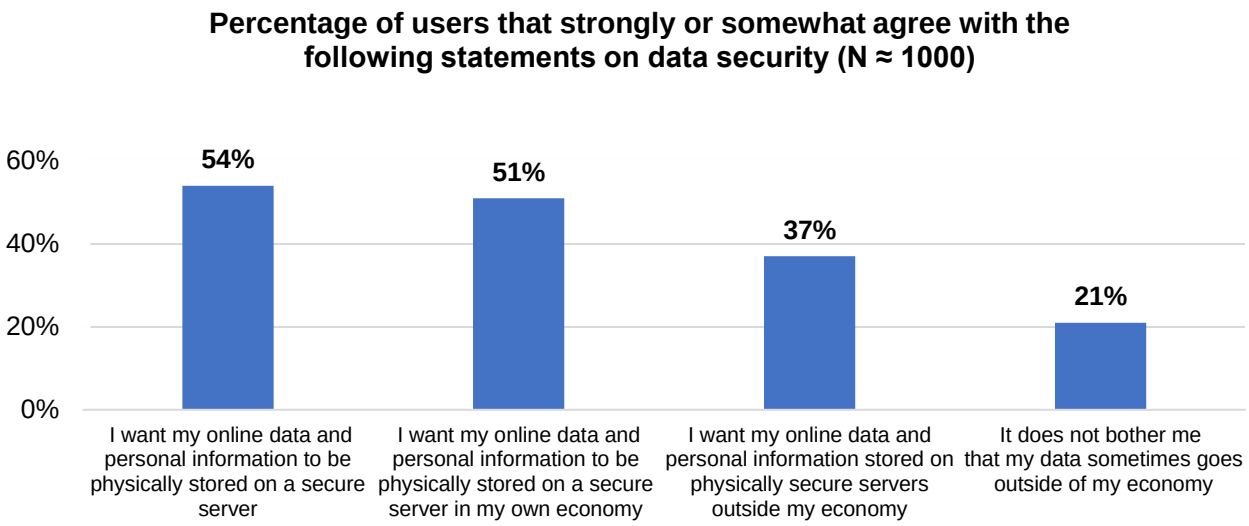

Fig. 7. Percentage of users that strongly or somewhat agree with the respective statements on data security (cf. CIGI-Ipsos, 2019b, pp. 13, 15, 17, 19, CIGI-Ipsos, 2019c, p. 283).

2. Concerns and Risks related to Data Control

About a quarter (23%) of the Japanese respondents report that they disclose fewer personal data online because they do not trust the Internet. Even fewer mention self-censoring what they say online (18%). 15% of the Japanese interviewees say they put more effort into securing their devices, and 13% use the Internet more selectively. Only 4% indicate they make fewer online purchases (cf. CIGI-Ipsos 2019c, p. 24) (Fig. 8).

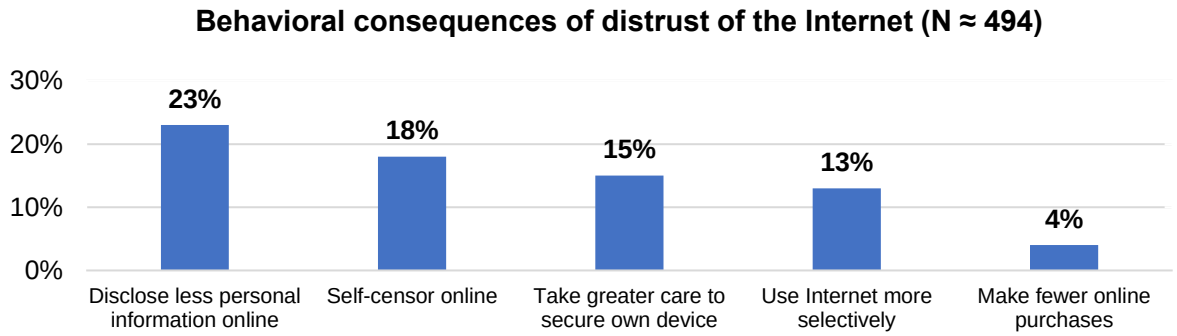

Fig. 8. Behavioral consequences of distrust of the Internet (cf. CIGI-Ipsos 2019c, p. 24).

VIII. Data Protection Literacy

[Data Protection Literacy] captures [Japanese 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.[30]

Only a small minority of Japanese respondents (16%) say that they are very or somewhat aware of the data protection and privacy rules of their country, while 84% report that they are not very or not at all aware of them (cf. CIGI-Ipsos 2019b, p. 8, 2019c, p. 281) (Fig. 9).

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

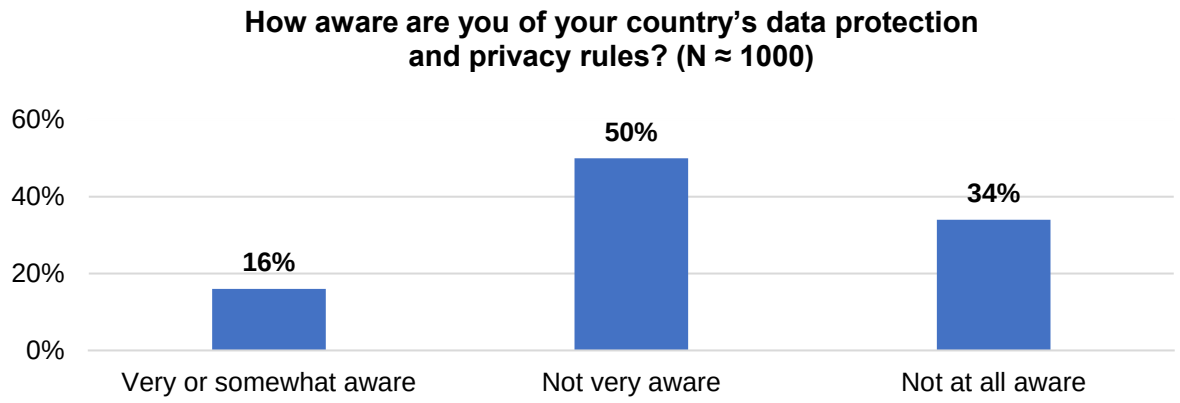

Fig. 9. Awareness of data protection and privacy rules in Japan (cf. CIGI-Ipsos 2019c, p. 281).

In another study, the percentage of Japanese respondents who say they are aware of privacy laws is only slightly higher, with a quarter (25%) indicating this (cf. Cisco 2021, p. 11). A majority (55%) of respondents from Japan, who said they knew the law, attribute a positive effect to Japan's Personal Information Protection Act (PIPA) (39% are neutral and 6% expect a negative effect) (cf. Cisco 2021, p.10).

About a third (35%) of Japanese respondents feel that they do enough to protect their own data (4% strongly and 31% somewhat agree) (cf. CIGI-Ipsos 2019b, p. 29, 2019c, p. 283).

IX. Attitudes Towards Data Receiver

[This] parameter […] refers to [Japanese 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.[31]

Trust towards others is somewhat low among Japanese respondents. A majority (61%) feels that most people cannot be trusted (cf. EVS/WVS 2021a, p. 7, 2021c, p. 174) (Fig. 10).

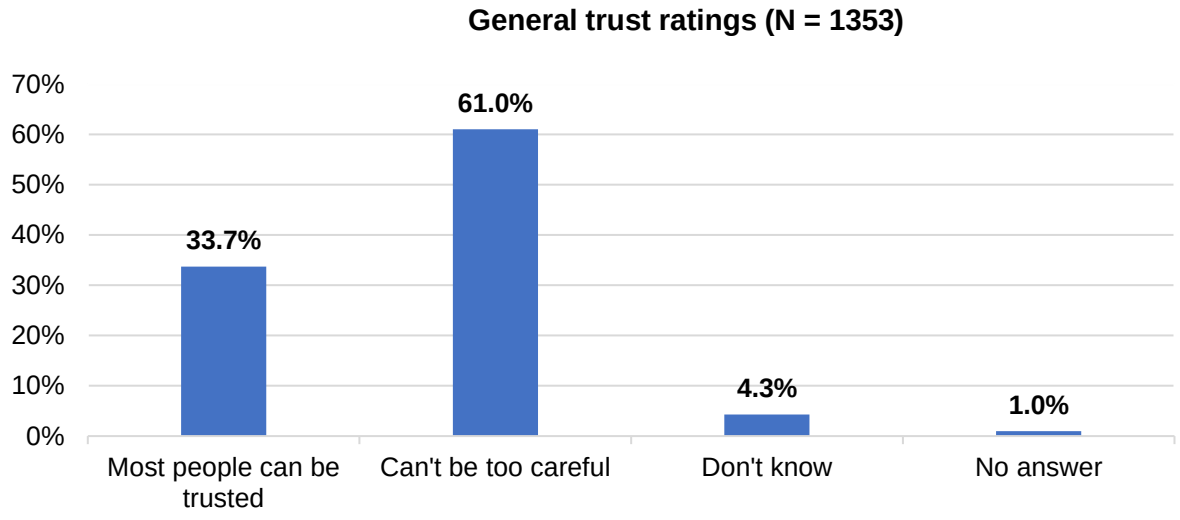

Fig. 10. Trust towards others in Japan (cf. EVS/WVS 2021c, p. 174).

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

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

1. Attitudes Towards Governments

Japanese respondents' attitudes towards their government and other political institutions reflect the prevailing distrust towards others. Majorities report that they do not really trust their government (52.1%), political parties (62.6%), and parliament (58.4%) (cf. EVS/WVS 2021c, pp. 266, 273, 275) (Fig. 11).

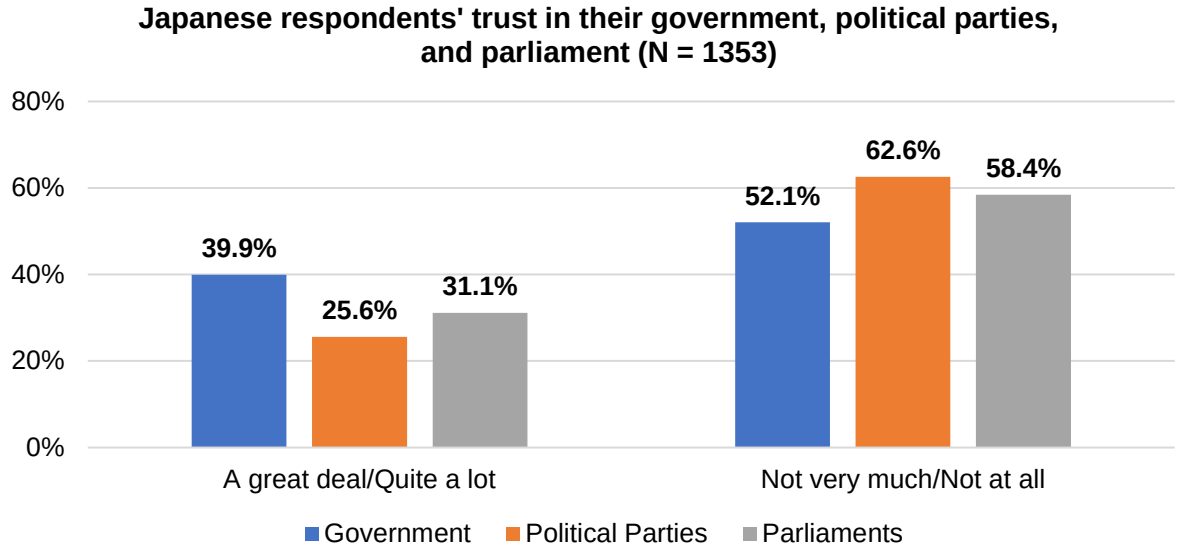

Fig. 11. Japanese respondents' trust in their government, political parties, and parliament (cf. EVS/WVS 2021c, pp. 266, 273, 275).

Moreover, only a little bit more than a quarter of the respondents from Japan (27%) agree (somewhat or strongly) that their government's efforts to protect their data are sufficient (cf. CIGI-Ipsos 2019c, p. 283). Japanese respondents' confidence that their government uses their personal data correctly is not very strong either: Only 37% trust their domestic government in this respect and even less, 13%, have confidence in foreign governments (cf. Ipsos 2019, p. 20) (Fig. 12).

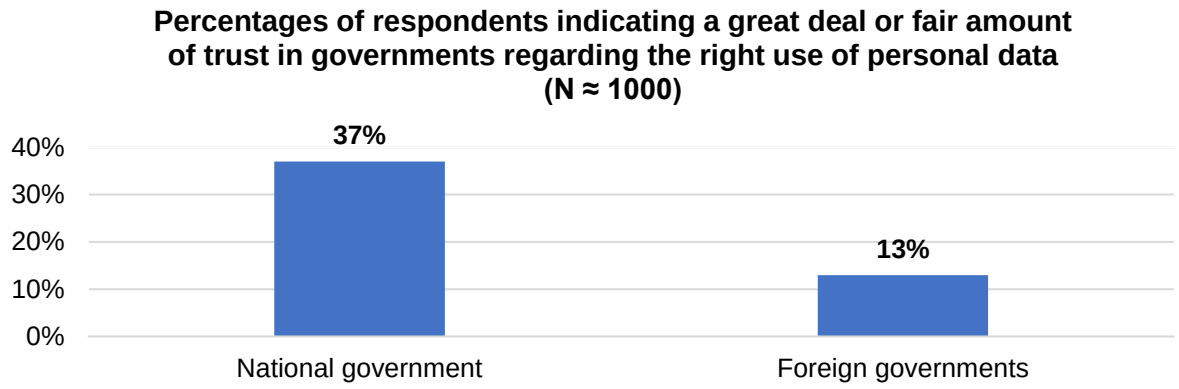

Fig. 12. Percentages of respondents indicating a great deal or fair amount of trust in governments regarding the right use of personal data (cf. Ipsos 2019, p. 20).

Besides, less than half of Japanese respondents (40%) report that their national government contributes to their distrust of the Internet, and 49% indicate this with regard to foreign governments (cf. CIGI-Ipsos 2019a, p. 117, 119, 2019c, p. 20) (Fig. 13).

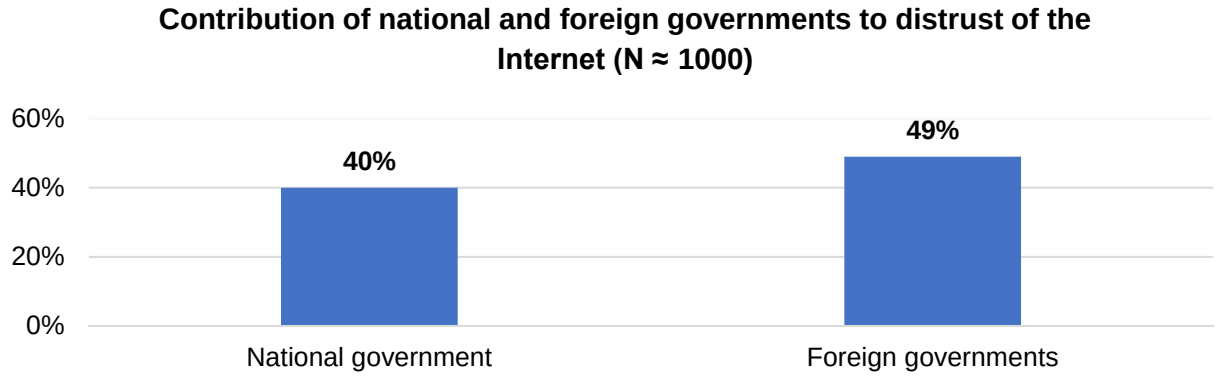

Fig. 13. Contribution of national and foreign governments to distrust of the Internet (cf. CIGI-Ipsos 2019a, pp. 117, 119, 2019c, p. 20).

2. Attitudes Towards Companies

The Japanese trust companies more than their government with their data: 37% of respondents think that companies do enough to protect their data, but only 27% agree that their government's efforts are sufficient in this respect (cf. CIGI-Ipsos 2019c, p. 283) (Fig. 14). Still, majorities think that neither companies nor their government does enough for data protection.

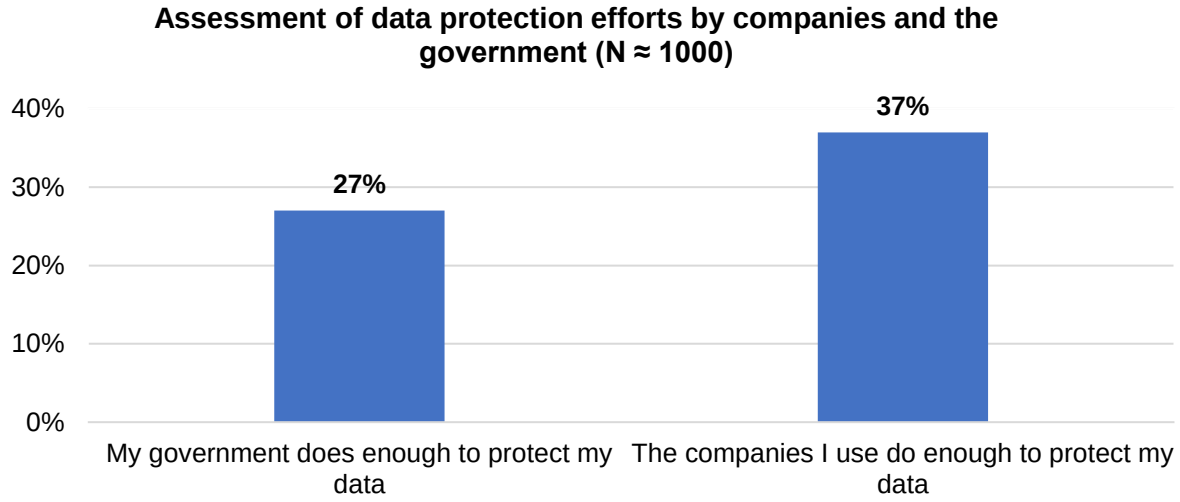

Fig. 14. Percentage of respondents that strongly or somewhat agree that companies' and their government's efforts suffice to protect their data (cf. CIGI-Ipsos 2019c, p. 283).

Japanese people's confidence in companies to use their data correctly varies when looking at different industries: A majority (57%) has confidence in healthcare providers (57%) and financial services companies (53%). All other sectors are trusted by less than 50% of respondents to handle their data properly: shipping and delivery companies (41%), retailers (37%), telecommunications companies (35%), search and social media sites (25%), and media companies (21%) (cf. Ipsos 2019, p. 20) (Fig. 15).

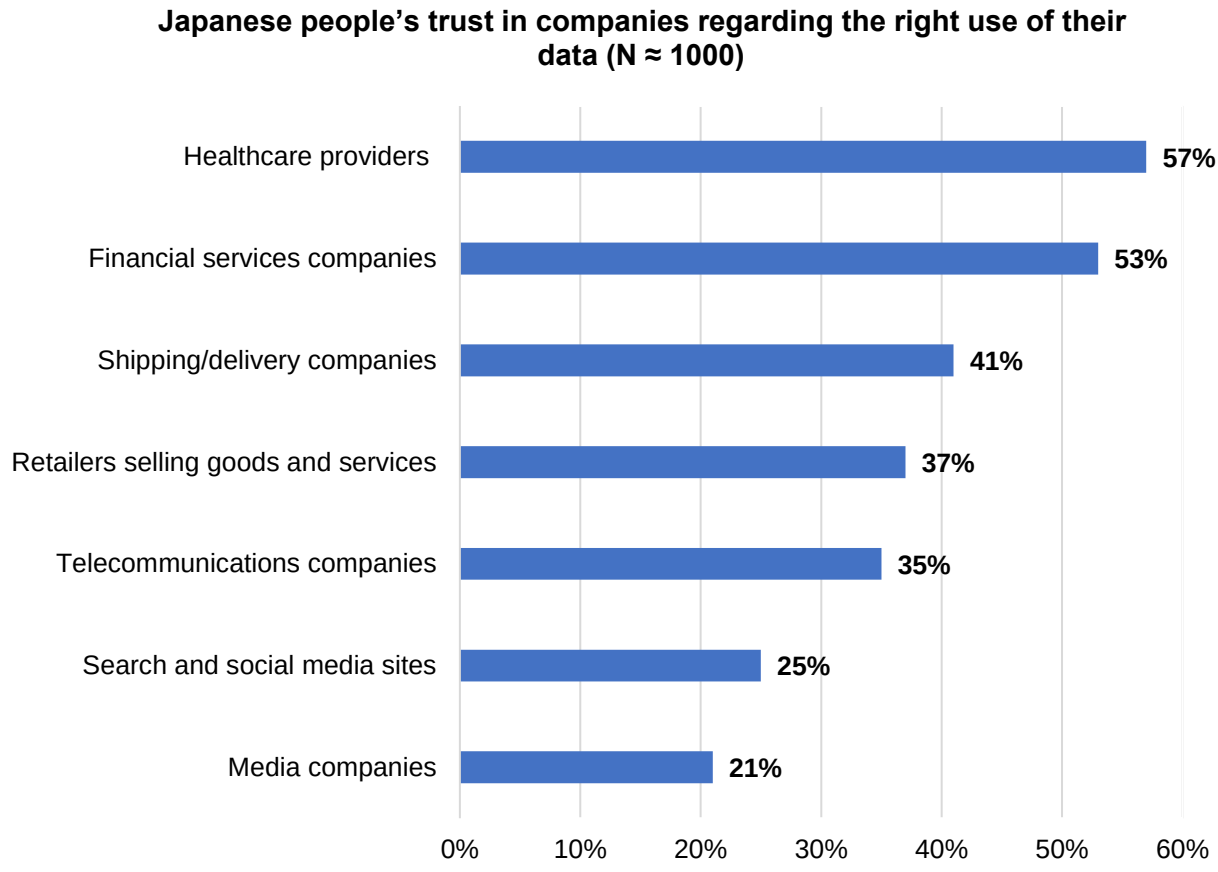

Fig. 15. Japanese people's trust in institutions regarding the right use of their data (cf. Ipsos 2019, p. 20).

Besides, the following institutions are reported to contribute to distrust of the Internet by respondents from Japan: social media companies (49%), search engines, online and mobile banking platforms (both 43%), Internet service providers (34%), and e-commerce platforms (33%) (cf. CIGI-Ipsos 2019c, p. 20) (Fig. 16).

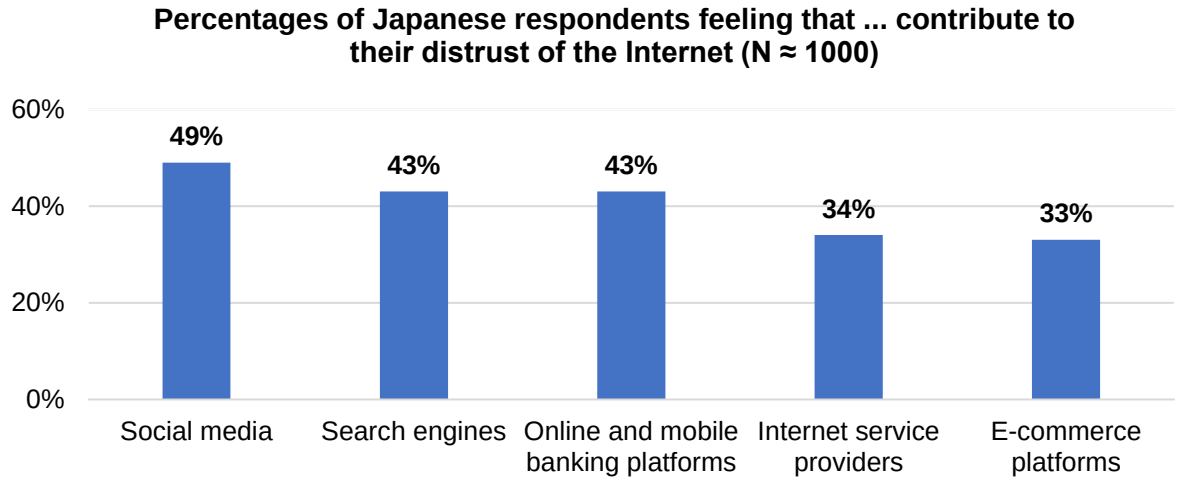

Fig. 16. Percentages of Japanese respondents feeling that the mentioned institutions contribute to their distrust of the Internet (cf. CIGI-Ipsos 2019c, p. 20).

X. Communication on Data Use

[This] parameter […] relates to the importance [Japanese respondents] attribute to communication on how their personal data are used.[32]

51% of Japanese respondents would rather give their personal data to companies that communicate transparently what the data will be used for. 48% 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).

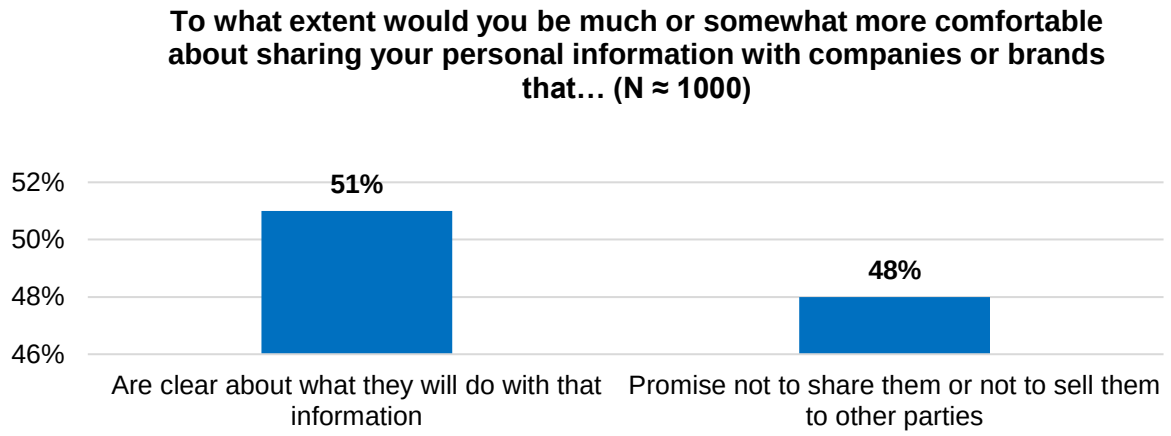

Fig. 17. Communication on data use (cf. Ipsos 2019, p. 14).

About a third (35%) of the respondents from Japan 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 Japanese people's WTS data (cf. Wawra 2022, IV. 3.).

1. Digital Competitiveness

In the *IMD World Digital Competitiveness Ranking* (IMD 2021), Japan is ranked 28th out of 64 countries for its overall performance with regard to digital competitiveness. It thus occupies a midfield position. It is also among the best half of all rated countries in all three main categories that indicate a country's digital competitiveness in the ranking: It ranks 25th for knowledge, 27th for future readiness for digitalization, and 30th for technology. These rankings have been relatively stable

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

over a five-year period. Japan's best rankings are in the field of future readiness for e-participation, where it ranks 4th, and for e-government, where it ranks 14th. In the category technology, it occupies 8th place for technological framework. Also, it ranks 13th in the field of knowledge for scientific concentration. Japan is ranked worst, however, in the knowledge subcategory talent (47th) and here particularly for personnel's digital and technological skills (62nd). In the category future readiness, it also only occupies rank 53 for business agility and here with rank 63 almost last place for the use of big data and analytics. 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 Japanese respondents consider governmental surveillance acceptable or not. A majority (57%) accepts governmental surveillance in public areas. However, only a minority approves of governmental email and Internet monitoring (22.4%) as well as secret data collection by the government in general (11.8%). Thus, informational privacy is assigned a significantly lower value in the context of state surveillance in the public sphere than in online environments, where it is highly valued by the vast majority of Japanese respondents. In addition, informational privacy is held in high regard by a clear majority when it comes to surreptitious state intervention.

Surveillance at work by technological means is accepted by less than a quarter (22%) of the Japanese respondents. Even less, 16% 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 small majority of Japanese respondents believe that consumers should have the right to refuse this (51%). A minority of respondents (41%) believe that consumers should be compensated for the use of their data. Only about a tenth of Japanese respondents (11%) does not mind companies using collected personal data.

We can deduce that, in the context of employer monitoring, informational privacy is a high priority for most of the Japanese respondents. A majority value their informational privacy as consumers. Only a minority of Japanese respondents believe that concessions to their informational privacy in this regard are worth compensation.

3. Degree of Privacy of Data

Sensitive personal data are usually referred to as sensitive personal information in legal texts in Japan. They can be used to identify a specific individual. According to the Japanese Act on the Protection of Personal Information (APPI), sensitive information comprises data on somebody's

- race
- creed
- social status
- medical history
- criminal record

as well as data on

- any crimes a person has been a victim of
- and any other information that might cause the person to be discriminated against.

The sensitivity ratings of Japanese respondents are highest for financial data (65%), followed by demographic data (55%) and medical data (52%), according to a survey that was conducted by Roose, Pang (2021). Fukuta et al. (2017) identify the following data – in declining order – as being above a medium privacy threshold (M > 2): ID numbers (M = 2.460 on a four-point Likert scale), financial information (M = 2.423), information on crimes, sensitive biometrics (both M ≈ 2.3), the digital persona (M ≈ 2.2), health and well-being (M ≈ 2.15), and contact numbers (M ≈ 2.1).

This reveals a significant discrepancy between the law and people's assessment of what constitutes sensitive data: Financial data, the most sensitive data according to Japanese respondents, are not (explicitly) included in the legal categories of sensitive data.

4. Benefits Associated with Data Disclosure

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

- companies to better tailor information, products, and services to their needs (27%)
- them as consumers to find relevant information, products, and services (28%)
- them as consumers save time (22%) and money (18%).

Thus, clear majorities do not consider any of these as benefits of data disclosure. Consequently, when asked directly about their willingness to disclose, not even a tenth of Japanese respondents (8%) 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. However, it did not differentiate between these different types of data either. As health data are sensitive personal data according to Japanese law, and as these and financial data have been categorized by a majority as sensitive or being above a medium privacy threshold (see Degree of Privacy of Data above), this could be an additional explanation for why an even larger majority of Japanese respondents indicate that they would not be very willing to share their data, even if they could expect to benefit from it: 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." 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 Japanese 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

Data security is not a really big concern for a majority of Japanese respondents. Only 45% would be more comfortable giving personal information to a company that has never experienced a breach, leak, or fraudulent usage of data. Moreover, a slight majority (54%) wants their data to be stored on a secure server, preferably in their own economy (51%). A minority wants their data to be stored abroad (37%), and merely 21% of the Japanese respondents do not mind if their data leave the country.

Consequently, an impeccable track record of data security is not expected to have a positive impact on the willingness of most Japanese respondents to share personal data. Secure data storage in their own country, on the other hand, is a way to score points with a majority.

b. Data Control

Because of their concerns about control over their data, less than one quarter of the respondents from Japan say they disclose less personal information online (23%) or self-censor what they say online (18%). 15% of the Japanese respondents indicate that they put more effort into securing their devices, 13% report that they use the Internet more selectively. Only 4% say they make fewer purchases online.

This can be interpreted as a manifestation of the privacy paradox (cf. Norberg et al. 2007, Barth, de Jong 2017, Wawra 2022, p. 2), as a majority of Japanese respondents are not more cautious in their data disclosure behavior despite existing privacy concerns. Nevertheless, 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 Japanese respondents.

6. Data Protection Literacy

Only a small minority of the respondents from Japan (16% to 25%, depending on the survey) are aware of the data protection and privacy rules that apply in their country. Of those who know the law, a majority (55%) attributes a positive effect to Japan's Personal Information Protection Act (PIPA). About a third (35%) reports that their efforts to protect their own data are sufficient.

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, Japanese respondents' trust in others is somewhat low with about a third (33.7%) saying that most people can be trusted and 61% expressing caution in this respect.

This is reflected in majorities of Japanese respondents not trusting political institutions either: 52.1% report that they do not trust their government very much or not at all, 62.6% say this for political parties, and 58.4% for parliaments. Even fewer respondents (27%) agree that their

government's efforts to protect their data are sufficient. Only a minority (37%) has confidence in their government that they use personal data correctly, and 13% trust foreign governments in this respect. In addition, minorities indicate that their national government (40%) and foreign governments (49%) 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 most Japanese people.

b. Attitudes Towards Companies

Only a minority (37%) of Japanese respondents consider the data protection measures of the companies they have done business with to be sufficient. Japanese people's trust in companies with regard to the proper use of their data varies, depending on the respective industry: A majority expresses their trust in healthcare providers (57%) and financial services companies (53%). For all other industries, trust rates remain below 50%, with 41% of the respondents indicating their trust in shipping/delivery companies, 37% in retailers, 35% in telecommunications companies, 25% in search and social media sites, and 21% in media companies. It can be deduced from this that for a majority of Japanese respondents, the WTS data is greatest towards healthcare providers and financial services companies.

Moreover, the following institutions contribute to Japanese people's distrust of the Internet (besides governments, see above): social media companies (49%), search engines, and online & mobile banking platforms (both 43%), Internet service providers (34%), and e-commerce platforms (33%).

8. Communication on Data Use

About half of the Japanese respondents would be more willing to disclose personal data if companies communicated the use of the data transparently (51%) and promised that they would not pass on the data (48%). About a third (35%) of the respondents indicate that it would also help if potential risks were communicated clearly. So, if companies convey transparently how they use people's data, this should potentially have a positive impact on the WTS data of a majority of Japanese respondents.

XII. Conclusion and Outlook

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

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

- the value Japanese respondents place on their informational privacy in different contexts
- what types of data are defined as sensitive personal data according to Japanese law and which data are considered more or less private or sensitive by Japanese 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 Japanese people place on data security
- reported behavior that follows from perceived privacy concerns and risks
- Japanese respondents' awareness of data protection and privacy rules and the evaluation of their own data protection efforts
- Japanese people's 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 Japanese 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).

Barth, S., de Jong, M. D. T. (2017). The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review. Telematics and Informatics 34(7). 1038-1058. DOI: 10.1016/j.tele.2017.04.013 (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: 12/03/2021).

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

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

EVS/WVS (2021b). European Values Study and World Values Survey: Joint EVS/WVS 2017-2021 Dataset (Joint EVS/WVS). JD Systems Institute & WVSA. Dataset Version 1.1.0. 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).

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).

Norberg, P. A., Horne, D. R., and Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs 41(1). 100-126. DOI: 10.1111/j.1745-6606.2006.00070.x (last access: 02/07/2022).

PwC (2021). Hopes and Fears 2021: Japan. https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2021/assets/pdf/hopes-and-fears-jp2021.pdf (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).

Unisys (2021). Unisys Security Index™: Global Report. https://www.unisys.com/unisys-security-index/ (last access: 01/08/2022).

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[33]

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 ≈[34] 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 the governmental and corporate ability to protect data.	N ≈[35] 1000	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 artificial intelligence (AI) and automated decision making." (p. 3)	N = 2600 in 12 countries	Age of respondents: 18+ No information on number of respondents from Japan
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 = 1762	Age of respondents: 18+ "random probability representative samples of the adult population" (EVS/WVS 2021)

[33] 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 Japan.

[34] 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).

[35] 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
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 = 1500	"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 ≈[36] 1000	Age of respondents: 16 - 64 "[…] results […] are balanced to reflect the general population" (Ipsos 2019, p. 21).
PwC (2021). Hopes and Fears 2021. Japanese Report	A survey of mainly workers' opinions in 19 countries about their current and future work situation	N = 1837	72% full time workers 14% part time workers 2% contract workers 12% self-employed business owners, students The sample size refers to the first three groups, the last group was not asked the questions that are rendered here.
Roose, J., Pang, N. (2021). Data Security, Privacy and Innovation Capability in Asia		N = 1020	"telephone-based survey interview" (Roose, Pang 2021, p. 3) Age 18-29 15% Age 39-29 14% Age 40-49 17%

[36] 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
			Age 50-59 15% Age 60 and above 39% Male 49% Female 51%