IRDG Institut für das Recht der digitalen Gesellschaft

UNIVERSITY OF PASSAU Faculty of Law

UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES NO. 22-04

CULTURAL INFLUENCES ON PERSONAL DATA DISCLOSURE DECISIONS

US-American Perspectives

Lena Kessel

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/

About the author

Lena Kessel conducts research on cross-cultural contexts of informational privacy and data disclosure.

Abstract

Findings from cross-national surveys predict cultural differences in privacy perceptions and aspects that might affect personal data disclosure. We summarize major findings within nine categories depicting factors that influence disclosure decisions. These categories comprise variables relating to digital competitiveness, the general value of informational privacy, the degree of privacy of data, benefits associated with data disclosure, privacy concerns and risks, data protection literacy, attitudes towards the data receiver, and the communication on data use. This paper focuses on the US specifically and serves as a basis for a cross-cultural comparison with other countries.

Cite as

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 No. 22-04*. https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/.

Keywords

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

Contents

I. Introduction[1]

This is one of several country reports that have been composed in our research project *Vectors of data disclosure – A comparative study of the use of personal data from a legal, cultural studies, and information systems perspective*[2], funded by the Bavarian Research Institute for Digital Transformation.[3] It focuses on cultural influences on people's willingness to share (WTS) personal data as expressed in surveys that reflect prevailing views, assumptions, attitudes, evaluations, and reported behaviors of US 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 the US. Our approach can be characterized as a macro level analysis (cf. Wawra 2022). We have composed similar 'reports' for other countries in our project, since we are planning a cultural comparative study as a next research step. This has also led to the decision to rely primarily on extensive global surveys in our reports to facilitate the following country comparisons. Secondarily, we have integrated surveys that cover at least some of our study countries. Wawra (2022) is an introduction to our project from a cultural perspective, which provides background information on the research context and details the cultural research design. The paper also introduces the parameters along which all of our cultural reports are structured. The following parameters have been identified as central to capture the narrower cultural context of data disclosure decisions on a macro level (cf. Wawra 2022): Digital Competitiveness (section III.), General Value of Informational Privacy (IV.), Degree of Privacy of Data (V.), Benefits Associated with Data Disclosure (VI.), Privacy Concerns and Risks (VII.), Data Protection Literacy (VIII.), Attitudes towards Data Receiver (IX.), and Communication on Data Use (X.) (see Figure 1). Data Protection Laws is another parameter that is detailed in separate legal country reports. Depending on the specific situational context, the parameters can all potentially have more or less influence on people's willingness to share (WTS) personal data. Overall, the structure of the country reports that have been compiled in our project is the same. The descriptions of the individual parameters have been adopted from Wawra (2022) and are rendered in italics.

[1] by Daniela Wawra.

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

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

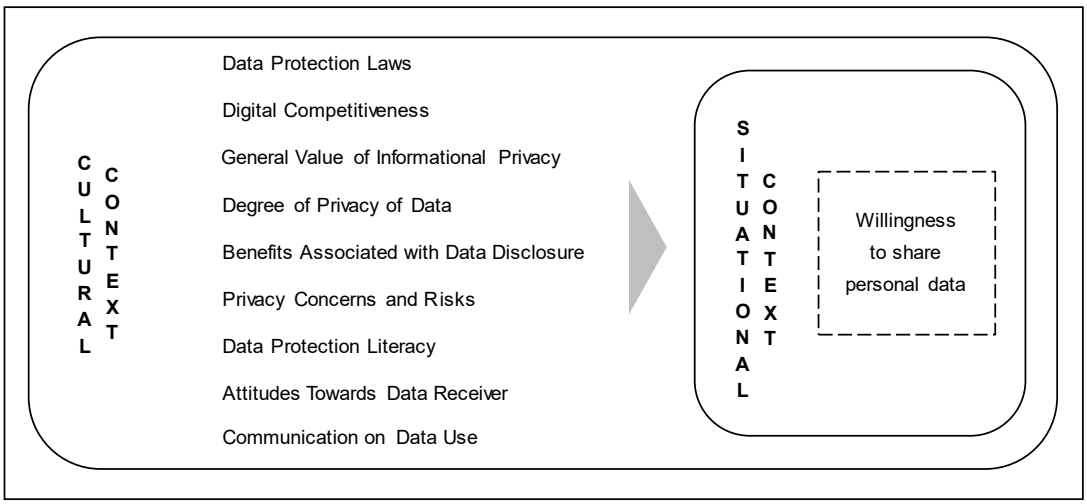

Fig. 1. Central parameters of data disclosure (from Wawra 2022).

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 the US. Appendix 1 gives an overview of the studies included and demographic details, i.e., countries of investigation, sample size, age of respondents, gender, education, socio-economic status, ethnicity, and political orientation.

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. 32). Knowledge describes the "[k]now-how necessary to discover, understand and build new technologies" (IMD 2021, p. 33) and is further divided into the sub-factors 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 sub-factors "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).

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

In 2021, the US has led the WDCR for the fourth year since it was first established in 2018 (c.f. IMD 2021, pp. 28, 172). As for factor rankings in 2021 specifically, the US received first rank in future readiness, they ranked third in knowledge, and fourth in the category technology (c.f. IMD 2021, p. 30).

As for future readiness, the US was especially strong in e-participation (use of online services that facilitate public's interaction with government), Internet retailing, tablet possession, and software piracy (percentage of unlicensed software installation, included in IT integration). Moreover, the US achieved a high score (third rank) for R&D activities (included among the sub-factor knowledge). Regarding "technology", the US achieved the highest ranking for issuing venture capital easily available for businesses. However, the United States scored low in the percentage of graduates in ICT, engineering, math and natural sciences (rank 56, training & education) (cf. IMD 2021, p. 173).

Concludingly, the US takes the global lead in motivating people to participate in online transactions, in fostering research, and in issuing venture capital for innovation. However, the US lays behind in educational topics, e.g., the amount of students that have a graduate degree in natural sciences or engineering (cf. IMD 2021, p. 173).

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 the US consider this demand].[5] The following surveyed questions allow for conclusions in this respect.

As for governmental surveillance, the World Values Survey (cf. EVS/WVS 2021b) has examined Americans' attitudes on this specific type of data collection. Americans seem to accept governmental video surveillance, whereas they reject online surveillance and data tracking without people's consent. A majority of 67.7% out of 2596 surveyed US-Americans agree that their governments should definitely or probably have the right to keep people under surveillance in public areas (cf. EVS/WVS 2021c, p. 428) (Fig. 2).

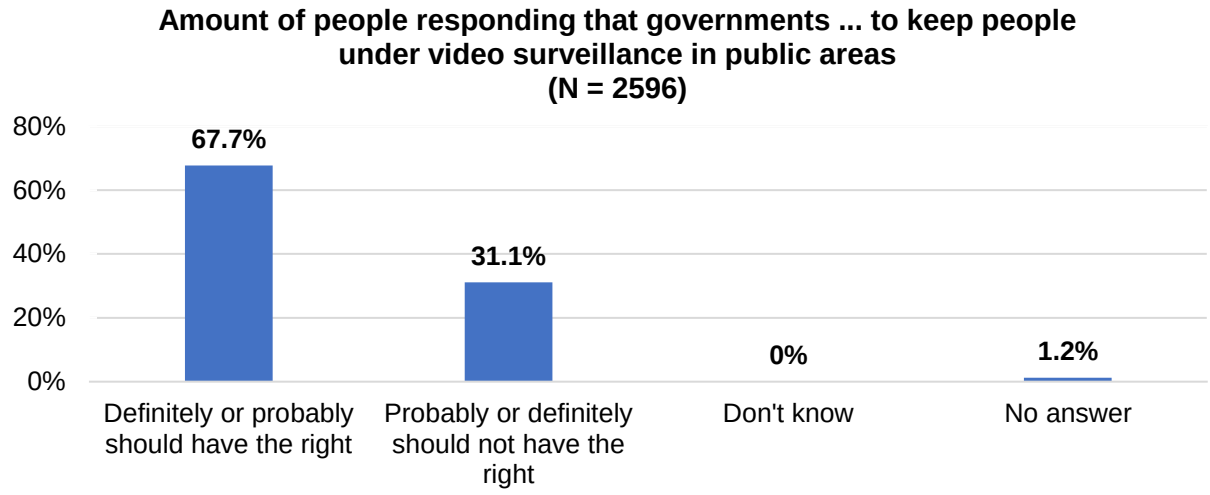

Fig. 2. Respondents' answers on governmental video surveillance (cf. EVS/WVS 2021c, p. 428).

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

In contrast, Americans seem to oppose email monitoring with a majority of 74.9% of Americans refusing that governments should have the right to monitor emails and any other information exchanged on the Internet (cf. EVS/WVS 2021c, p. 430) (Fig. 3).

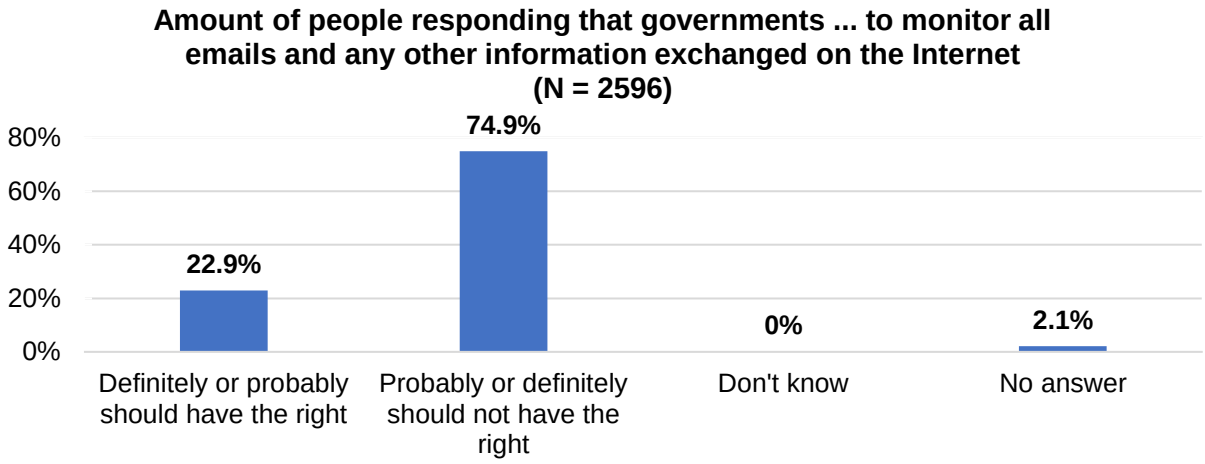

Fig. 3. Respondents' answers on governmental email-monitoring (cf. EVS/WVS 2021c, p. 430).

Americans' opinions towards governmental data tracking without people's consent equally represent an opposing attitude with 70.3 % responding that governments 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. 432) (Fig. 4).

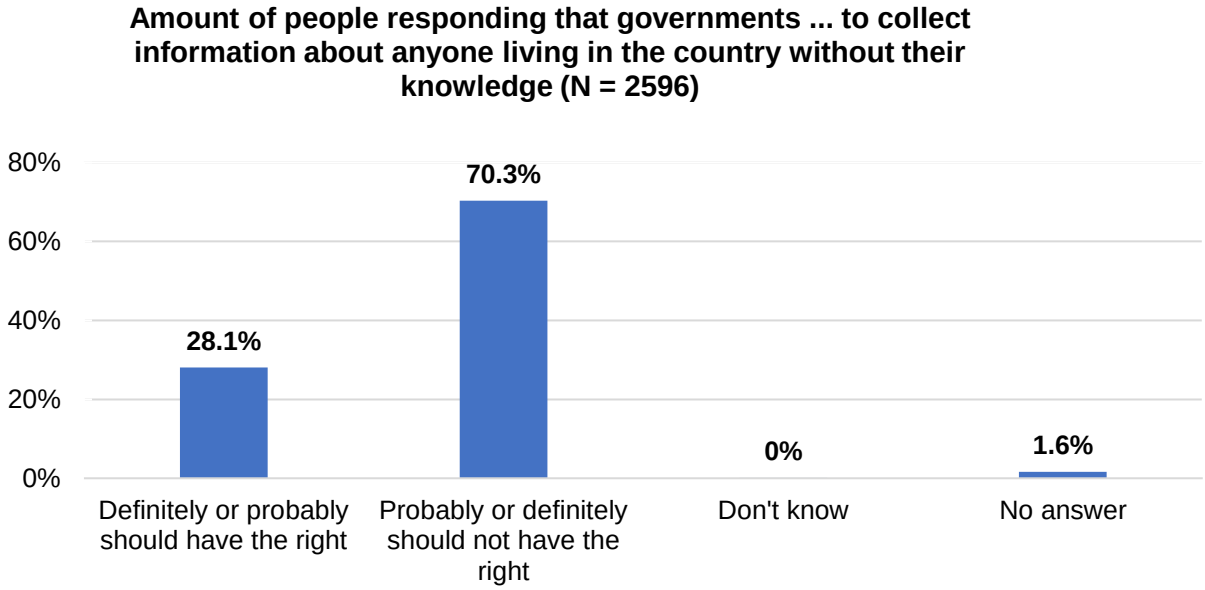

Fig. 4. Respondents' answer on governmental surveillance in terms of data tracking without consent (cf. EVS/WVS 2021c, p. 432).

75% of approximately 1000 US-American respondents somewhat or strongly agree that consumers should be able to refuse that companies use collected data. Moreover, a majority of Americans (61%) believe that consumers should be paid or rewarded in return for the use of their data. Only a minority of 23% of American respondents do not bother about companies' use of collected data (cf. Ipsos 2019, p. 12), indicating that most Americans do care about what is happening to their data (Fig. 5).

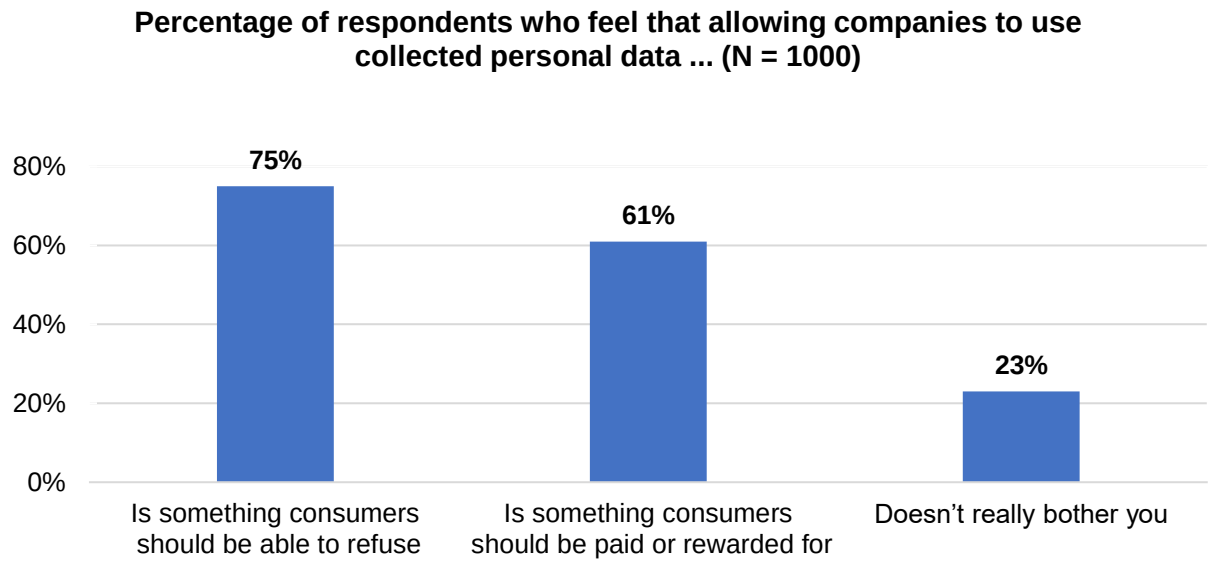

Fig. 5. Attitudes towards allowing companies to use collected personal data (cf. Ipsos, 2019, p. 12).

Regarding surveillance in the workplace, Americans seem to largely accept that employers use technology to monitor performance at work (cf. Madden 2017b, p. 120) (Fig. 6).

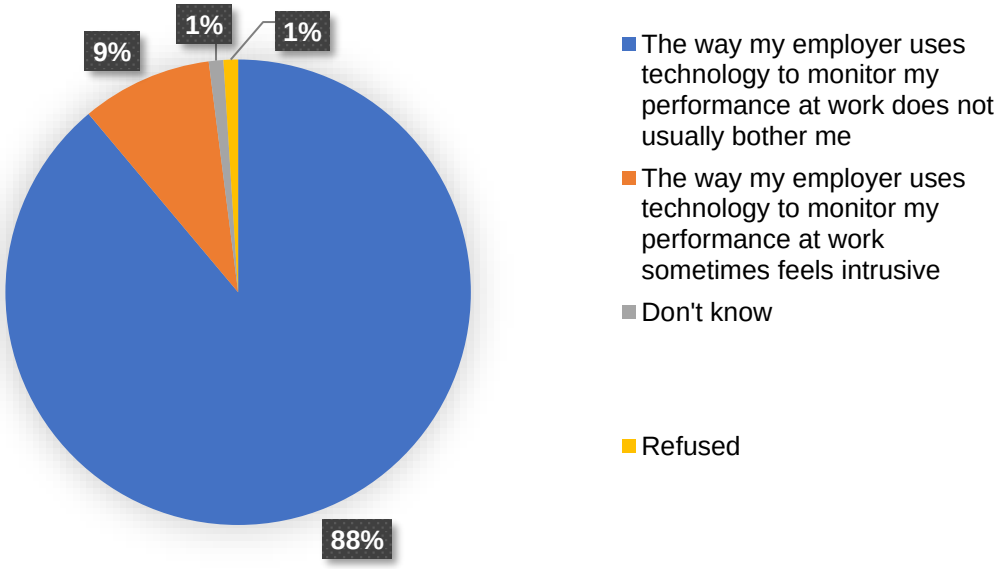

Fig. 6. Responses regarding the question "Which of the following statements comes closest to describing how you feel about the way your employer uses technology to monitor your performance at work, even if neither is exactly right?" (N = 714) (cf. Madden 2017b, p. 120).

V. Degree of Privacy of Data

[This] parameter […] surveys how private or sensitive […] certain kinds of personal data [are for US respondents].[6]

Trepte and Masur (2016) asked for "the extent to which participants considered different kinds of information to have the potential to affect their privacy. We presented them with different

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

behaviors (e.g., telling your relationship status, telling your political orientation, telling your sexual orientation, and having an open profile), and participants had to indicate the extent to which this kind of information affected their privacy. Possible answer options ranged from 1 (does not affect my privacy at all) to 5 (affects my privacy very much)" (Trepte and Masur 2016, pp. 61, 62). Mean values (M) show that US-American respondents (N = 555) feel that telling their relationship status (M = 2.42), their political orientation (M = 2.27), or their sexual orientation (M = 2.3) does rather not affect their privacy. Only having an open profile is considered as a scenario that has a higher impact on privacy (M = 3.74) (cf. Trepte and Masur 2016, p. 62). Trepte and Masur (2016) also adapted a scale on the sensitivity of specific pieces of information, developed by Jourard & Lasakow (1958), to explore how survey respondents feel about the degree of privacy of, e.g., feelings about their own sexuality, records of illness, etc. (Fig. 7).

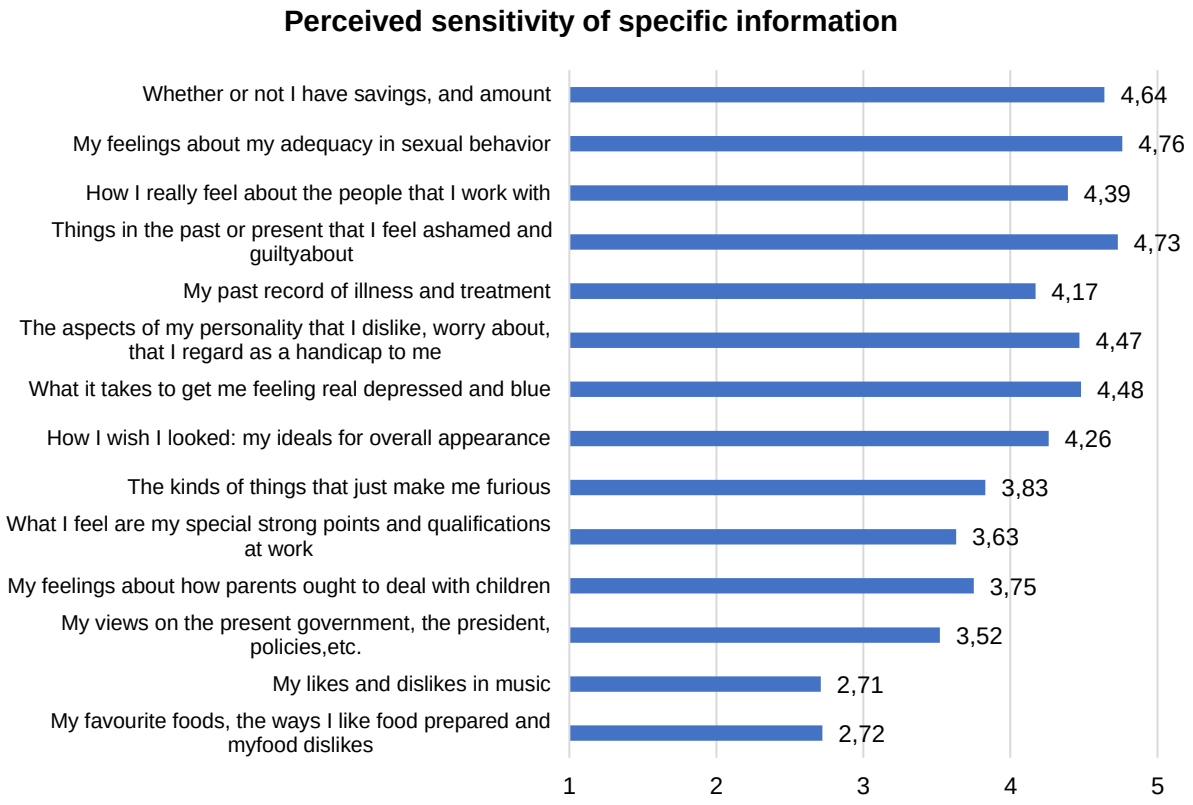

Fig. 7. Perceived sensitivity of specific pieces of information (cf. Trepte and Masur 2016, p. 63).

Results indicate that Americans are most sensitive about information on their "[f]eelings of adequacy" of their "sexual behavior" (4.76 on a 7-Point Likert Scale), what they "feel ashamed and guilty about" (4.73), and their savings (4.64).

VI. Benefits Associated with Data Disclosure

[This] parameter […] renders the positive effects [US respondents] expect from the disclosure of their personal data.[7]

Saving time and money, discovering relevant products that fit one's needs, and providing products, services, and information that better fit consumers' needs are among the benefits that are associated with data disclosure to companies (cf. Ipsos 2019, p. 12). Whilst less Americans value savings in

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

time (34%) and money (28%), more value that data disclosure helps them finding and providing relevant products, services, and information (44%) (Fig. 8).

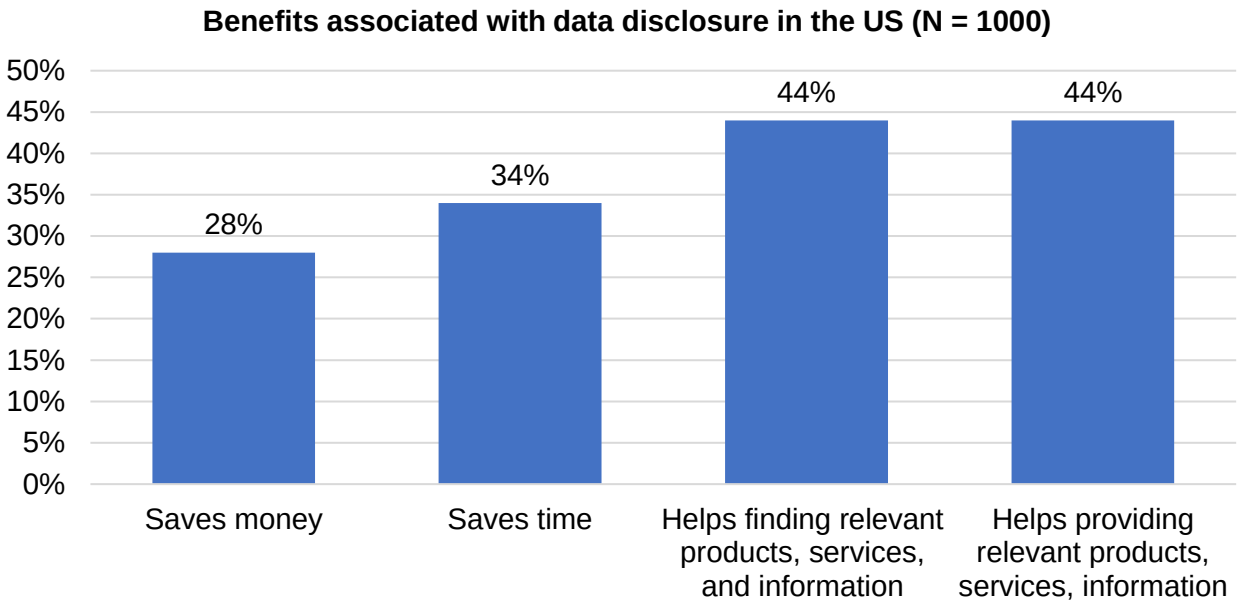

Fig. 8. Benefits associated with data disclosure in the US (cf. Ipsos 2019, p. 12).

Furthermore, Americans seem to consider compensation in return for their data as a benefit that would make them more comfortable in disclosing their information. A majority of 66% out of 1000 American survey respondents agree that they would be more comfortable about sharing their personal information with companies or brands that offer compensation in return for their data (cf. Ipsos 2019, p. 14).

Associated benefits with data disclosure also become evident in altruistic contexts. Americans especially point to the value of data disclosure if, e.g., non-profit groups use data to improve educational programs in poorly performing schools, or to prevent terrorist attacks. In contrast, less find it acceptable to allow social media monitoring for users' signs of depression or allowing law enforcement to access smart speaker recordings for criminal investigations (see the full list of relevant contexts in Fig. 9) (cf. Auxier et al. 2019, pp. 6, 7, 8).

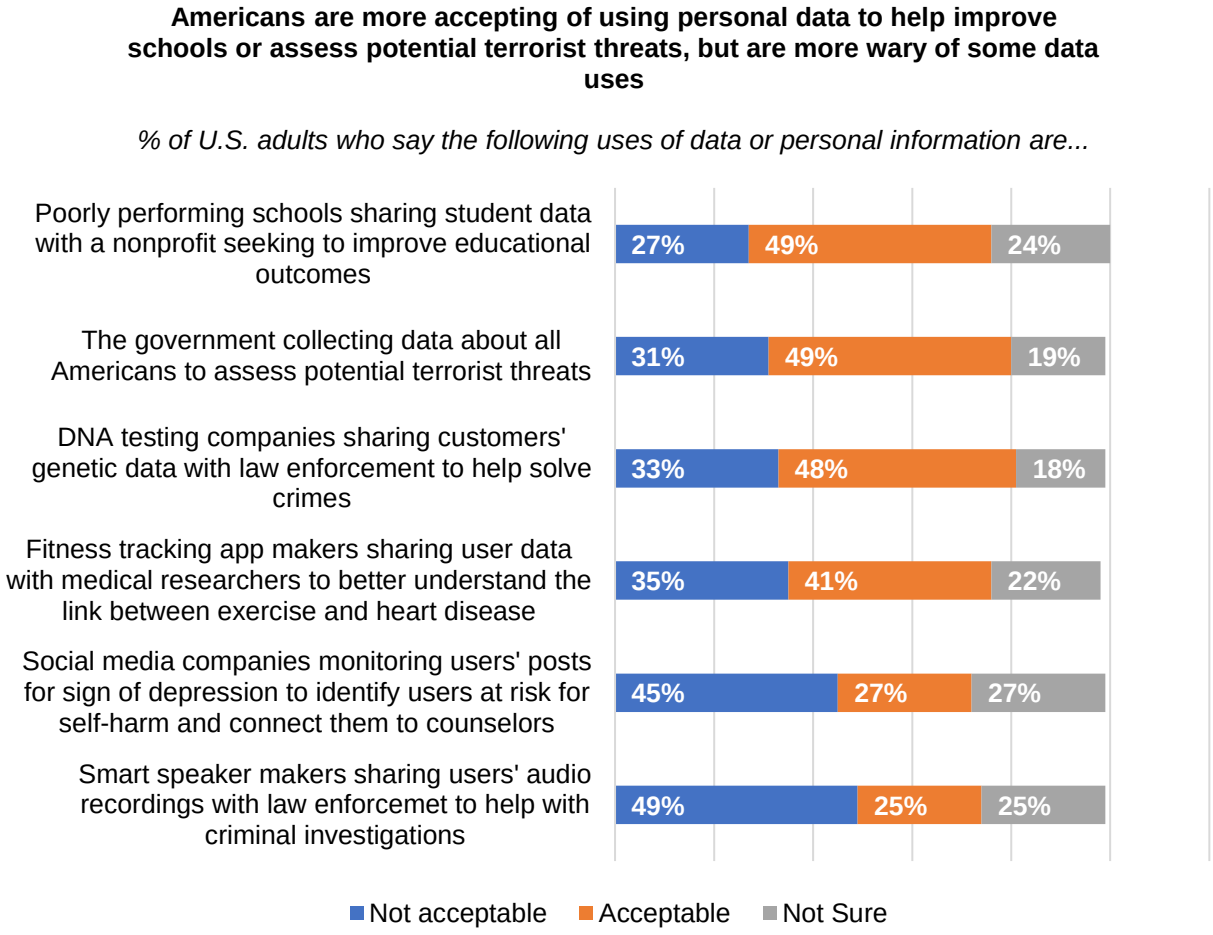

Fig. 9. Acceptance of data disclosure in diverse contexts (cf. Auxier et al. 2019, p. 8).

Regarding demographic differences, younger Americans (ages 18–29) are more likely to acknowledge benefits of data disclosure to governments or companies than Americans aged 65 and older. Specifically, younger survey respondents are more likely to accept social media monitoring for signs of depression to advertise adequate treatment opportunities (42% vs. 18%), and to allow fitness tracking apps to share their data with researchers that work on links between exercise and heart disease (52% vs. 35%) (cf. Auxier et al. 2019, p. 35). Conversely, older survey respondents are more likely to accept that law enforcement agencies use genetic data to solve crimes (58% vs. 39%), collect data to monitor terrorists (54% vs. 42%), or use data from smart speakers for criminal investigations (32% vs. 22%) (cf. Auxier et al. 2019, pp. 36).

Overall and despite the illustrated benefits of data disclosure, a minority of 2140 surveyed Americans agree that they benefit from data disclosure to companies (28%) or the government (23%) (cf. Auxier et al. 2019, p. 28). Splitting this result by social groups, younger people (ages 18-29) tend to see data disclosure as more beneficial than older ones, especially compared to respondents aged 65 and older (29% vs. 19% companies/ 32% vs. 17% governments) (Fig. 10).

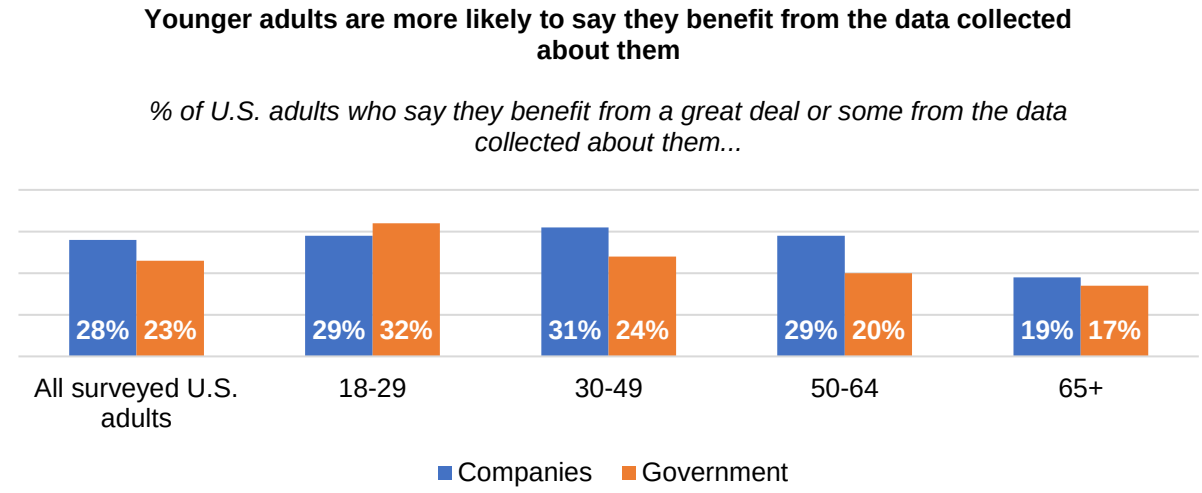

Fig. 10. Age differences regarding the benefits of data collection (cf. Auxier et al. 2019, p. 29).

Overall, a majority of surveyed Americans indicate that risks of disclosing data to companies (17% of 2140) or governments (31% of 2132) outweigh benefits (Fig. 11).

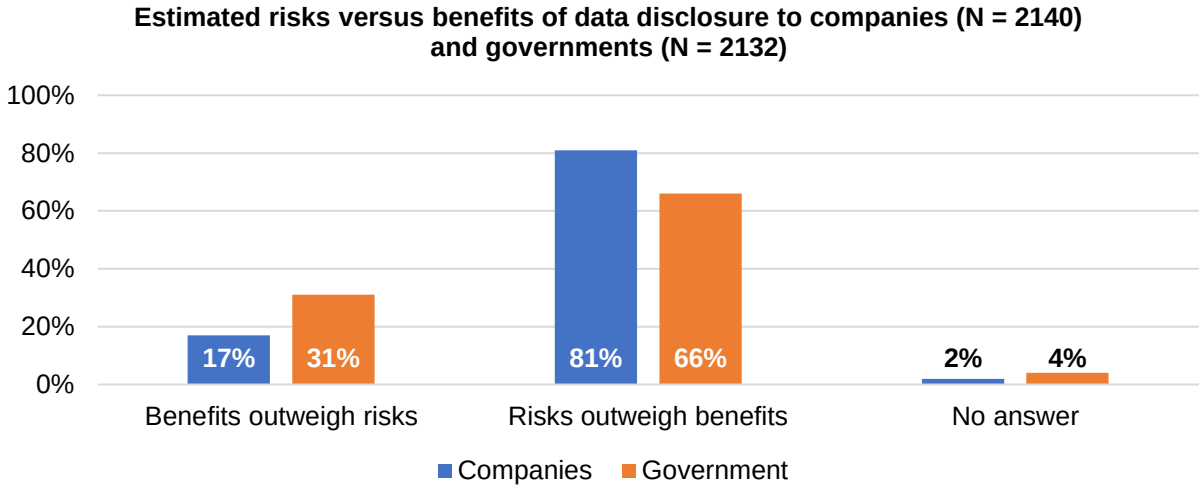

Fig. 11. Americans' assumptions on risks vs. benefits of personal data disclosure (cf. Auxier et al. 2019, 53, 55).

VII. Privacy Concerns and Risks

[This] parameter […] comprises the negative effects [US respondents] associate with data disclosure. These include their general concerns about the security of their personal data, and their control over them.[8]

1. Concerns about Data Security

Results from two large surveys indicate that more Americans believe that their data has become less secure during the last five years (cf. Auxier et al. 2019, p. 15; Olmstead & Smith 2017, 3, 34). Olmstead and Smith (2017) indicate that 49% of 1040 surveyed Americans "feel that their personal information is less secure than it was five years ago" (Olmstead & Smith 2017, p. 3) compared to

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

18% that feel that their data has gotten more secure, and 31% do not indicate a difference to the past (cf. Olmstead & Smith 2017, p. 3). Auxier et al. (2019) even observe that 70% of 4272 surveyed Americans feel that their data is less secure today than five years ago (cf. Auxier et al. 2019, p. 15). Specifically, Americans are concerned about being the victim of an Internet scam or fraud (59% indicate being very/somewhat concerned; N = 3000) and about not knowing what personal information is being collected by companies and about how companies use this information (73%) (Madden 2017a, pp. 102, 103). Overall, Americans who follow privacy news more closely (74%) seem to be somewhat more concerned about data security than five years ago compared to the ones not reading news on privacy (64%) (cf. Auxier et al. 2019, p. 18).

Negative experiences with data breaches may have increased Americans' doubts about data security throughout the past five years. About three in five Americans indicate that they have been affected by security threats (cf. Olmstead & Smith 2017, pp. 2, 3). Overall, 64% have experienced some sort of data theft. 41% of 1040 surveyed Americans have experienced security breaches in terms of fraudulent charges on their credit or debit cards, 35% have received a notice that their personal information had been stolen, and 15% had to deal with compromised social security numbers. In addition, 16% of 926 Internet users had their e-mail accounts taken over without permission, 14% of 665 social media users had a loan or line of credit taken out in their name, 13% had their social media accounts taken over without permission, and 6% indicated that others took out their tax refunds in their name (cf. Olmstead & Smith 2017, 9, 35) (Fig. 12).

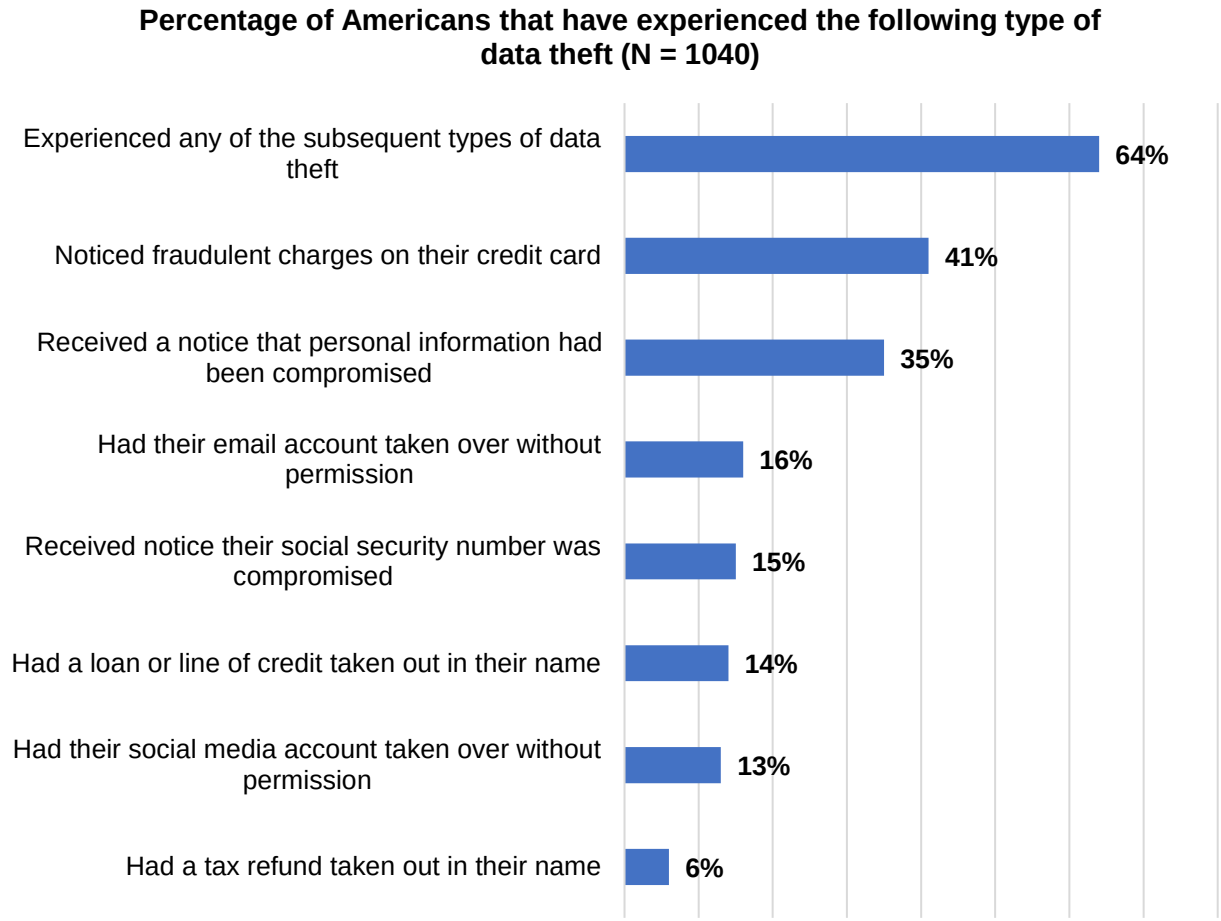

Fig. 12. Percentage of Americans that have experienced a certain type of data theft (cf. Olmstead & Smith 2017, 9, 35).

Data breaches seem to decrease the willingness to disclose data to companies. Asked to what extent respondents would be more comfortable about sharing their personal information, a majority of 59% (N ≈ 1000) answers that they are much or somewhat more comfortable with sharing their data with companies that have never been subject to any breach, leak, or fraudulent usage of data (cf. Ipsos 2019, p. 14).

Regarding demographic differences, people older than 50, richer people (income more than $75,000 a year), and people with a college degree tend to be slightly more likely to indicate that data security has decreased (cf. Auxier et al. 2019, p. 16) (Fig. 13).

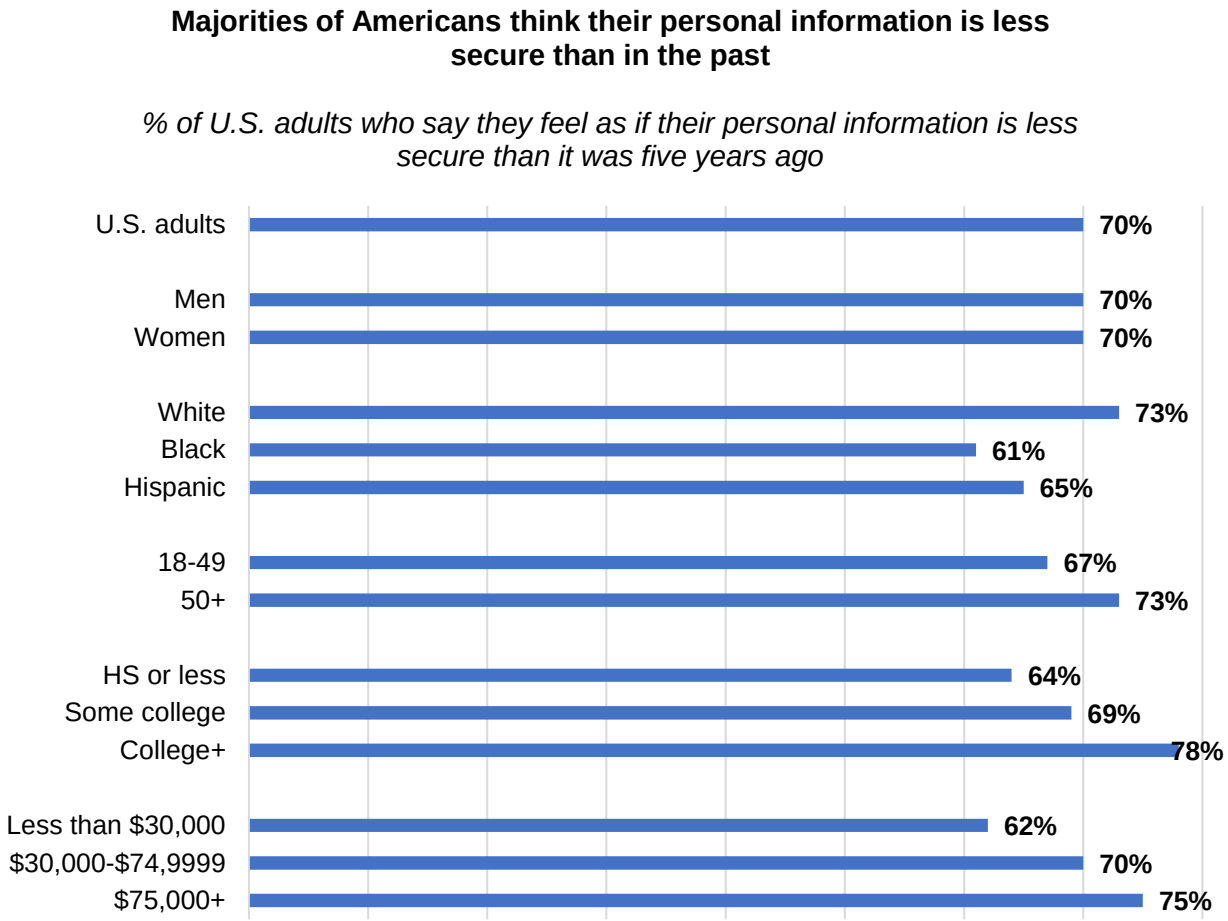

Fig. 13. Percentage of respondents indicating that data is less secure than five years ago (cf. Auxier et al. 2019, p. 16).

Regarding security breaches, adults ages 30 to 60, college graduates, and high-income households ($75,000 or more per year) are most likely to indicate that they have experienced at least one of the previously mentioned types of data breaches. For example, 48% of adults between 30 and 60 have experienced fraudulent charges on their credit cards, and 78% of college graduates and 77% of high-income households indicate that they have faced at least one of the previously mentioned data breaches (cf. Olmstead & Smith 2017, p. 10).

Americans' wish to store their data on secure servers reflects their demand for data security. 70% of 1000 surveyed Americans want their data to be stored on a secure server, preferably within the US (as indicated by 73% of American respondents). Only 24% would accept data storage abroad and a minority (27% to 31%) agrees that they would not be bothered about data that leaves the US

(Fig. 14). Overall, the results indicate that Americans tend to worry about what happens to data that is stored outside domestic boundaries.

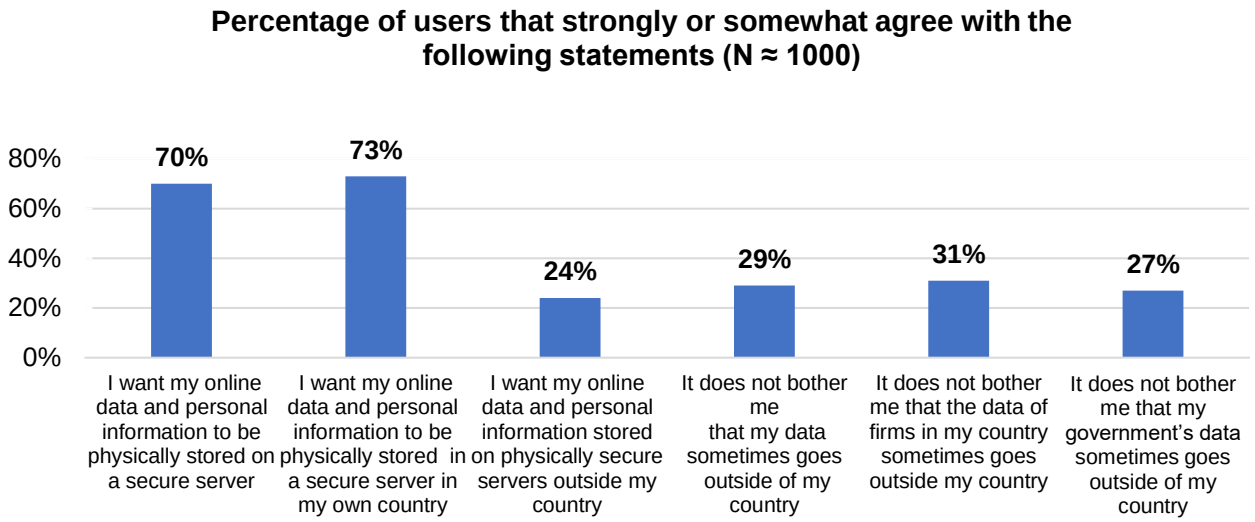

Fig. 14. Percentage of users that strongly or somewhat agree with the respective statements (cf. CIGI-Ipsos 2019b, pp. 13, 15, 17, 19, 21, 23, 2019c, p. 283).

2. Concerns about Data Control

Most Americans indicate concerns on how companies use their data (79% of 2140 respondents indicate they are somewhat or very concerned) (cf. Auxier et al. 2019, 21, 52). Specifically, Americans mention concerns about what social media sites (85% of 1778 respondents), advertisers (84% of 2140 respondents), and "companies they buy things from" (Auxier et al. 2019, p. 21) (80% of 2132 respondents) know about them (cf. Auxier et al. 2019, p. 21).

Moreover, Americans mention concerns about what law enforcement (62% of 2140 respondents), employers (58% of 1313 respondents), families and friends (43% of 2132 respondents) (cf. Auxier et al. 2019, 21, 56), and governments (64% of 2132 respondents) may know about them (cf. Auxier et al. 2019, p. 54).

About six in ten Americans tend to believe that they cannot "go through daily life" (Auxier et al. 2019, p. 2) without being tracked by governments or companies (cf. Auxier et al. 2019, 2, 55). Especially the group of young adults aged 18 to 29 is more aware of online data tracking than the ones aged 65 and older. Whereas 60% of the former believe that governments track their cellphone activities, only 30% of the latter do so (cf. Auxier et al. 2019, p. 26).

Specifically, a large amount of American Internet users claim that they have no or little control over who can access search terms they use online (87% of 2140 American Internet users) or websites they visit (85%). In addition, 88% of 2140 respondents claim having no or little control about data tracking on the purchases they make online or in person, and 82% claim the same for data on their physical location. Furthermore, 85% out of 1800 social media users indicate having little or no control about others' access to their posts or activities on social media (cf. Auxier et al. 2019, p. 6). In line with low perceived control over social media content, Trepte and Masur (2016) report that Americans also associate relatively high risks with an open social media profile (M = 3.78 on a 5-Point Likert Scale) and with uploading pictures (M = 3.62) (cf. Trepte & Masur 2016, pp. 40, 41).

The perception of control over the use of personal data also seems to vary between age. Americans ages 65 and older indicate less control over access to their personal information than adults ages 18 to 29 (e.g., access to physical location, online and offline purchases, or conversations with others) (cf. Auxier et al. 2019, p. 10).

Regarding ethnic groups, respondents' perception of control depends on the institution that is collecting data. On the one hand, White Americans seem to worry more about corporate data collection than Hispanic and Black Americans: Only 50% of White American adults think they can control who can find out what they bought on- and offline, compared to 66% of Hispanic and 69% of Black adults (cf. Auxier et al. 2019, p. 11). On the other hand, Black adults seem to be more skeptical towards governmental data collection, i.e., 60% think that the government is tracking their cellphones compared to 43% of White and 56% of Hispanic Americans indicating the same (cf. Auxier et al. 2019, p. 26).

Overall, the results indicate that Americans are aware of data tracking and a majority seems to believe that it is impossible to live without being tracked. That older people mention less control over access to their data may relate to less experience with and less knowledge of digital technologies. As younger ones have grown up with digital tools, they tend to be more familiar with technologies and more confident about managing their privacy settings. In addition, skepticism towards governmental data collection across Black communities may be increased by the strong media presence of movements like *Black Lives Matter* that stand up for institutional injustice Black communities face frequently (cf. Black Lives Matter 2021).

Behavioral consequences of general privacy concerns when using the Internet have been surveyed by the Center for International Governance Innovation and Ipsos Public Affairs (CIGI-Ipsos) (cf. CIGI-Ipsos 2019a). Most American respondents indicate that they disclose less information online as a result of distrusting the Internet (52% of 1000). Almost half of the respondents further indicate that they take greater care in securing their devices, because they distrust the Internet (43% of 1000). Less mention that they use the Internet more selectively (38%), self-censor what they say online (35%), or make fewer online purchases (18%) (Fig. 15).

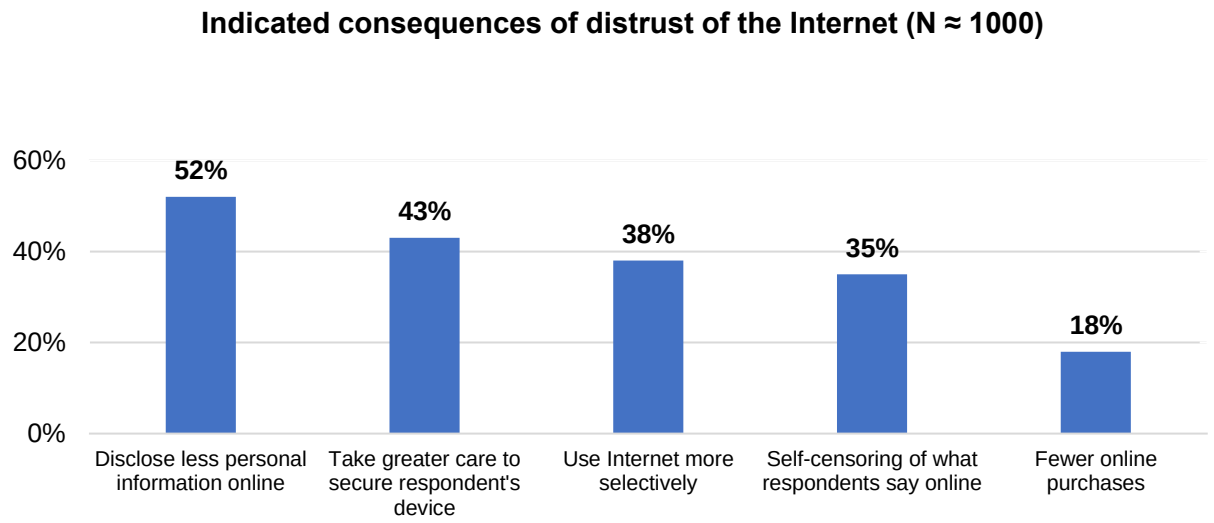

Fig. 15. Consequences of distrust of the Internet (cf. CIGI-Ipsos 2019c, p. 24).

VIII. Data Protection Literacy

[Data Protection Literacy] captures [Americans'] 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.[9]

Overall, Americans' awareness of institutional data protection and privacy rules seems rather low, with a minority being very or somewhat aware of data protection and privacy rules (33% out of 1000 surveyed respondents) (cf. CIGI-Ipsos 2019b, p. 8, 2019c, p. 281) (Fig. 16).

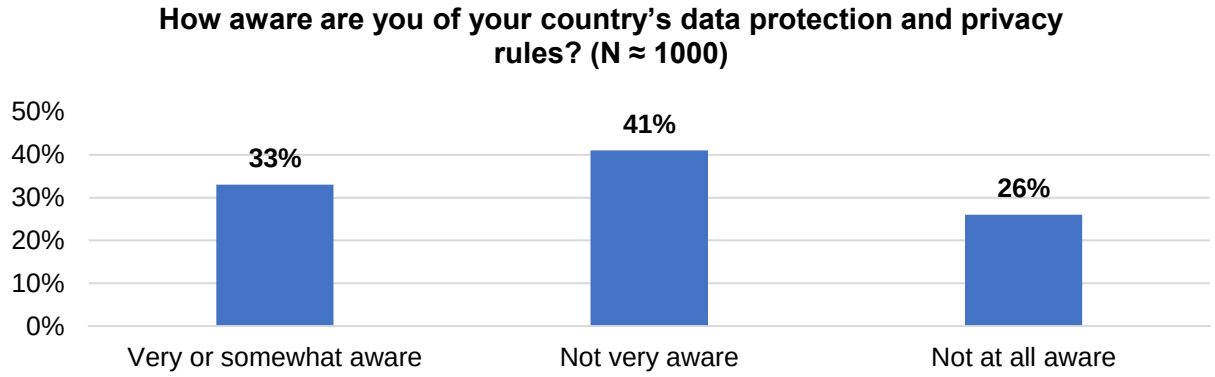

Fig. 16. Awareness of data protection and privacy rules in the US (adapted from CIGI-Ipsos 2019c, p. 281).

Americans' knowledge of topics related to data protection and privacy seems low as well (cf. Madden, 2017 p. 52; Vogels & Anderson 2019, p. 4). While a majority of 4272 US adults (57%) say they follow privacy news very closely (11%) or somewhat closely (46%) (cf. Auxier et al. 2019, p. 10), the picture is different, when it comes to understanding existing data laws: A minority of the 4272 respondents say they understand a great deal of data regulations (3%) or some of it (33%), whereas a majority indicates understanding very little (49%), or nothing at all (14%) about data protection laws (cf. Auxier et al. 2019, 41, 59). Moreover, only a minority understands what companies or governments do with the data they collect (cf. Auxier et al. 2019, p. 10). 6% of 2140 respondents feel they understand a great deal about what companies use their data for, and 34% mention some understanding, whereas most respondents indicate very little (48%) or no knowledge (11%) about what companies are doing with their data (cf. Auxier et al. 2019, pp. 52, 53).

The number of respondents who say they read privacy policies before giving their consent to disclose personal data is low as well. Only 9% of 4170 respondents always, 14% often, and 39% sometimes read privacy policies before agreeing to them, whilst 37% admit that they never read privacy policies. When asked "When you read a privacy policy, what do you typically do?" (Auxier et al. 2019, p. 57), 22% (of 2571 respondents) indicate reading the policies all the way through, 35% read at least parts of it, and 43% say they "glance over it without reading it closely" (Auxier et al. 2019, p. 57).

Results of a digital knowledge quiz conducted by the *PEW Research Center* illustrate examples for the lack of understanding of privacy-related topics. Only 30% of 4272 American respondents correctly answered that the "s" in "https://" stands for encrypted information (Vogels & Anderson 2019, 4, 13). Regarding knowledge on private browsing features, 49% of 4727 surveyed Americans indicated that they were not sure about the implications of private browsing features, whilst only

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

24% knew that private browsing can restrict a coworker on the same computer from seeing online activities of the person browsing in private mode (cf. Vogels & Anderson 2019, p. 14).

In contrast to these findings, i.e., overall, rather low awareness, knowledge, and understanding of data protection and privacy, most Americans express confidence in their data protection skills. A majority of 60% of 1000 surveyed Americans express their confidence in doing enough to protect their own data (12% strongly and 48% somewhat agree) (cf. CIGI-Ipsos 2019b, p. 29, 2019c, p. 283). Madden (2017) even reports that Americans seem overconfident about their skills to protect their privacy and suggests a desirability bias that may obscure respondents' true skills (cf. Madden 2017a, p. 53). Specifically, respondents say they tend to restrict online posts to open audiences by using privacy settings (65% of 2350 surveyed American Internet users), they avoid communicating online if they have to share sensitive information (56%), they turn off cookies (52%), or they deter from using websites that ask for real names or email addresses (51%) (cf. Madden 2017a, p. 52) (Fig. 17).

Yet, other privacy practices appear less popular. Only 31% seem to use search engines or web browsers that do not track user activity. Even less install ad blocking software (24%), anonymize their browsing activities by using VPNs (22%), use apps like Snapchat that automatically delete messages (20%), or utilize fake photos (19%) or inaccurate profile information (18%) to disguise their online activities (cf. Madden 2017a, p. 62) (Fig. 17).

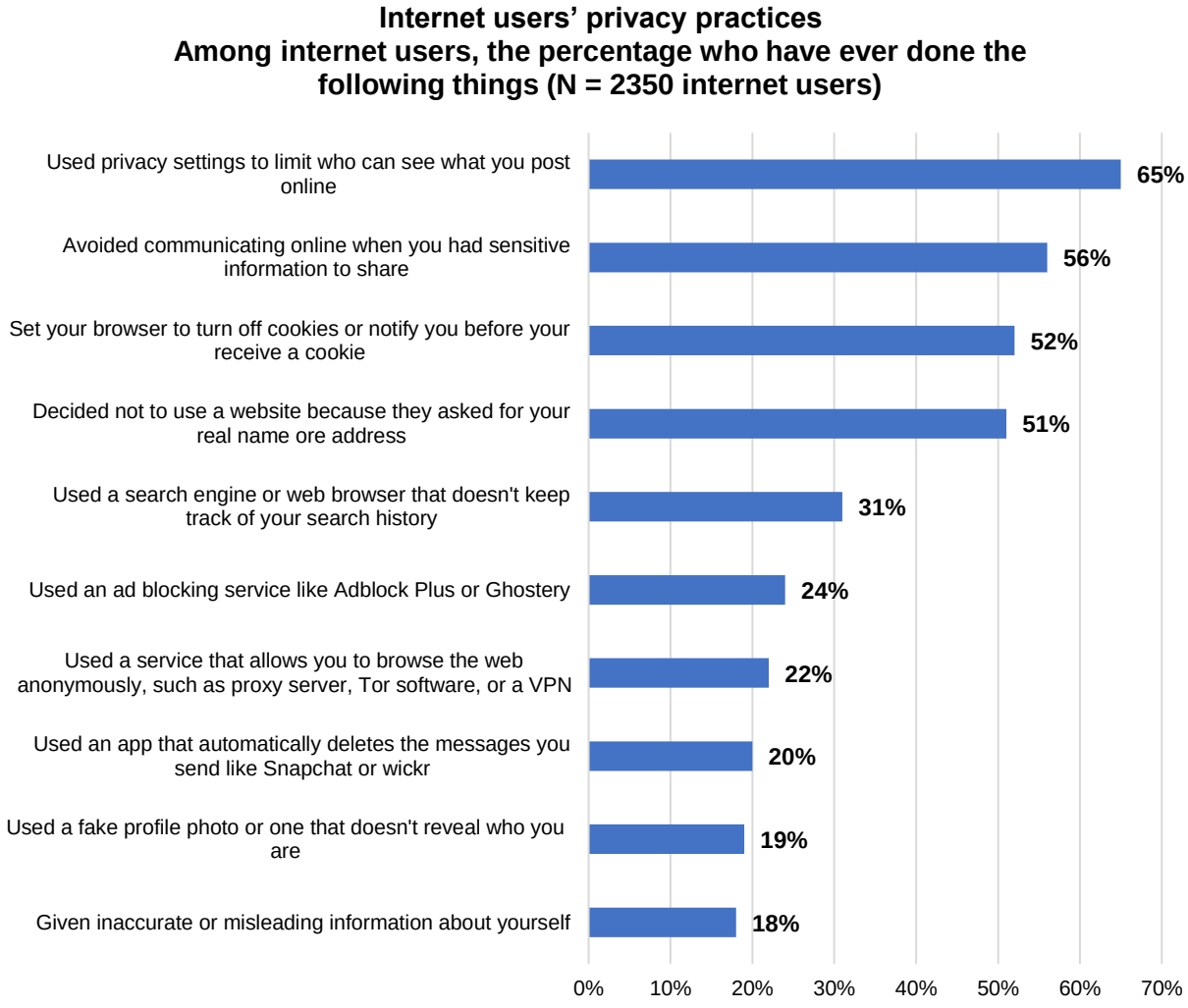

Fig. 17. Internet users' privacy practices (adapted from Madden 2017a, p. 62).

Data protection literacy varies between demographic groups, i.e., between men and women, younger and older adults, groups of diverse educational backgrounds, income, and ethnicity. Moreover, differences occur between rather urban and rural populations.

Regarding knowledge about data protection and privacy, younger adults (aged 18-49) seem to know more about certain topics related to privacy protection than older ones (aged 50+). Younger participants taking part in the digital knowledge quiz were able to answer a median number of five out of ten questions correctly whereas respondents older than 50 only got a median of three questions right. The largest differences between youngest (age 18-29) and oldest survey participants (age 65+) became visible in knowledge about private browsing functions. Whilst 42% of people aged 18-29 knew that private browsing mode only prevents someone using the same computer from seeing one's online activities, only 8% of respondents older than 65 answered correctly (cf. Vogels & Anderson 2019, p. 6).

Education also seems to affect knowledge about data protection and privacy. 54% of the surveyed Internet users with less than a high school degree express their confidence in knowing enough about privacy settings, whereas 78% of Internet users with a college degree feel confident about using privacy settings (cf. Madden 2017a, 56-57). In addition, adults without college education seem to know less about specific questions related to data protection than adults with a college degree. Results of a digital knowledge quiz indicate that only 34% of 1483 respondents with no college degree knew that privacy policies represented contracts between website providers and users on how user data are utilized, whereas 64% of 1600 respondents with at least a bachelor's degree knew about the contractual character of privacy policies (cf. Vogels & Anderson 2019, p. 5). Regarding the "s" in "https://", 17 % of respondents without any college experience knew the right answer, whereas 47% of the right answers were given by college graduates (cf. Vogels & Anderson 2019, p. 5).

The degree of knowledge about privacy settings also varies between groups of different income. Americans with an income below $20,000 per year are somewhat less likely to express their confidence in knowing enough about privacy settings than Americans earning at least $20,000 a year. 61% of 396 respondents earning less than $20,000 indicate knowing enough about privacy settings, whilst 73% of Internet users earning at least $20,000 express confidence in knowing how to manage their privacy settings (cf. Madden 2017a, p. 56–57; 109).

Regarding ethnic backgrounds, foreign-born Hispanics (29%) are the ones least likely to know enough about managing privacy settings, compared to 75% of White, 63% of Black, 75% of US-born Hispanics, and 76% of non-Hispanic Internet users (N= 2350) indicating they already know enough about managing privacy settings for information they share online. They are also the ones most likely to ask for more education on managing privacy settings (67% of foreign born Hispanics vs. 32% of Black respondents, 21% of White and 24% of US-born Hispanic respondents) (cf. Madden 2015, p. 328, 2017a, 52; 56-57). Regarding privacy rules in particular, 71% of foreign-born Hispanic Internet users would like to better understand the privacy policies of websites and applications, compared to only 21% of White, 34% of Black, and 23% of US-born Hispanics (cf. Madden 2015, p. 333, 2017a, 57-58).

When it comes to applying measures to protect one's privacy, women are somewhat more likely to use privacy settings to restrict public access to online posts than men (69% of surveyed women use privacy settings versus 61% of men) (cf. Madden 2017a, p. 63). Moreover, women (65%) are more likely to read privacy policies than men (55%) (cf. Auxier et al. 2019, p. 38).

Regarding age, the largest gaps exist between those aged 18-29 (77% say they use privacy settings), and people older than 64 (32%). In between, 71% of respondents aged 30-49 use privacy settings, and 60% of those aged 50-64 (cf. Madden 2017a, p. 63).

Americans with lower levels of education (less than a college degree) seem to be less likely to apply privacy measures than respondents who completed an academic degree. The survey data indicates that only 49% of Internet users without a college degree say they use privacy settings, whereas 72% of users with a college degree do so. Considering other measures to protect one's privacy, people with less than a high school degree (37%) are less likely to deter from sharing sensitive information online than the ones with a college degree (66%) (cf. Madden 2017a, p. 64). Regarding cookie settings, differences between educational groups become even more pronounced. Whilst 31% of respondents with less than a high school degree report that they turn off cookies, 63% of users with a college degree indicate that they restrict cookies to protect their privacy (cf. Madden 2017a, p. 65).

Variations between income groups (below and above $20,000 per year) show that respondents with lower incomes (57%) are less likely to use privacy settings than respondents with higher incomes (67%). In a similar vein, respondents from low-income groups are more prone to communicate sensitive information online whereas high-income respondents rather deter from online communication if sensitive information could be tracked (52% vs. 63%) (Madden 2017a, p. 64). Moreover, 37% in lower-earning households indicate that they tend to turn off cookies to protect their privacy, compared to 63% of households earning more than $40,000 (cf. Madden 2017a, p. 65).

Varying use of privacy settings also becomes evident among ethnic groups, especially between White Americans and foreign-born Hispanics living in the US. Whilst 68% of White Americans indicate using privacy settings, only 44% of foreign-born Hispanic Internet users do (cf. Madden 2017a, p. 63). Additionally, White Internet users are more likely to avoid online communication on sensitive topics than foreign-born Hispanics (59% vs. 36%) (cf. Madden 2017a, p. 65). Considerable gaps between White Americans and foreign-born Hispanics living in the US also appear when respondents indicate that they adjust cookie settings as a privacy strategy. While 53% of White American respondents adjust their cookie settings, only 26% of foreign-born Hispanics indicate the same (cf. Madden 2017a, p. 65).

Ultimately, respondents from rural ares (56%) are slightly less likely to use privacy settings than respondents that access the Internet in urban (65%) or suburban areas (67%) (cf. Madden 2017a, p. 63)

Overall, the findings on data protection literacy suggest that a majority of Americans is not very aware of and does not know a lot about data protection, privacy rules, and policies. At the same time, most of the respondents consider their skills and the measures they take to protect their personal data as sufficient. Indeed, certain privacy settings like restricting posts to certain communities or hiding sensitive information seem quite popular whereas others, e.g., using additional services like add blockers are rarely used.

Moreover, the knowledge about data protection and the application of privacy practices varies between demographic groups. Education, income, and ethnicity seem to especially affect data protection literacy in the sense that people with lower levels of education and lower income, as well as foreign-born Hispanics seem to be the ones least aware of data protection, and least likely to apply measures to protect their privacy. In addition, variations in data protection literacy have been revealed to exist between women and men, younger and older respondents, as well as between people living in rather urban or rural areas. Women are slightly more likely to apply privacy settings than

men, younger people are more likely to take measures to protect their privacy than older ones, and people living in urban areas rather use privacy protection than the rural population.

IX. Attitudes Towards Data Receiver

[This] parameter […] refers to [Americans'] 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.[10]

Generally, trust towards other people in the US seems low. When respondents were asked whether most people can be trusted or whether they should be very careful in dealing with people (cf. EVS/WVS 2021a, p. 7), a majority of Americans (62.5%) indicate that one can't be too careful in dealing with people (Fig. 18).

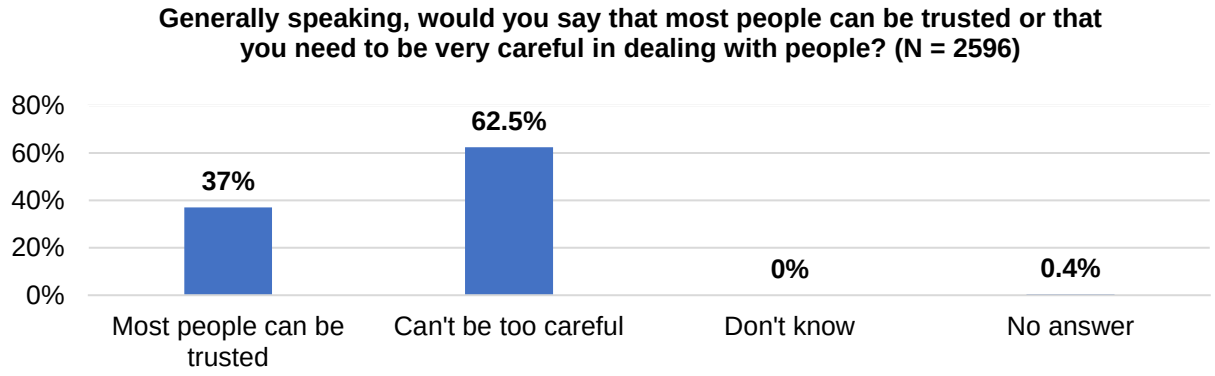

Fig. 8. General trust towards people in the American society (cf. EVS/WVS 2021c, p. 175).

The statistics indicate that a lot of Americans distrust others in general, which might also affect how people disclose their personal information. The following chapters further elaborate Americans' attitudes towards their governments and companies in the specific context of data disclosure.

1. Attitudes Towards Governments

Americans' attitudes towards governments mirror low levels of trust in governmental institutions in general, and specifically with regard to data protection. Findings from the World Value Survey (cf. EVS/WVS 2021c, pp. 267, 274, 276) indicate that a majority of American respondents does neither express confidence in their governments, nor in political parties or parliaments (Fig. 19).

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

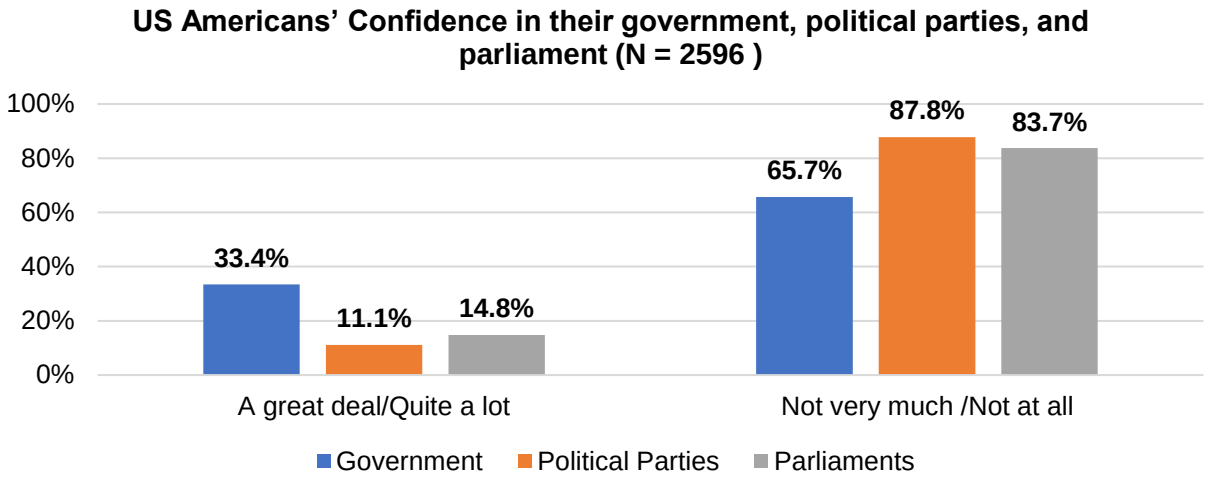

Fig. 9. Americans' confidence in their government, political parties, and parliament (cf. EVS/WVS 2021c, 267, 274, 276).

Further survey findings indicate that only 35% of 1000 US respondents strongly or somewhat agree that their governments do enough to protect their data (cf. CIGI-Ipsos 2019c, p. 283). Conversely, 75% of 2140 surveyed Americans think that there should be more governmental regulation whilst only 8% call for less regulation, and 16% say it should be "about the same amount" (Auxier et al. 2019, p. 59). Especially Democrats call for more government regulation, with 81% calling for more regulatory measures whereas 70% of Republicans do so. Moreover, people who follow privacy news more closely also seem to be more likely to call for more regulation (cf. Auxier et al. 2019, 43).

Trust in how governments use personal data also seems to be low in the US. 34% of 1000 surveyed respondents indicate that they trust their national government in using personal information in the right way. As for foreign governments, trust rates are lower and only reach 16% (Fig. 20).

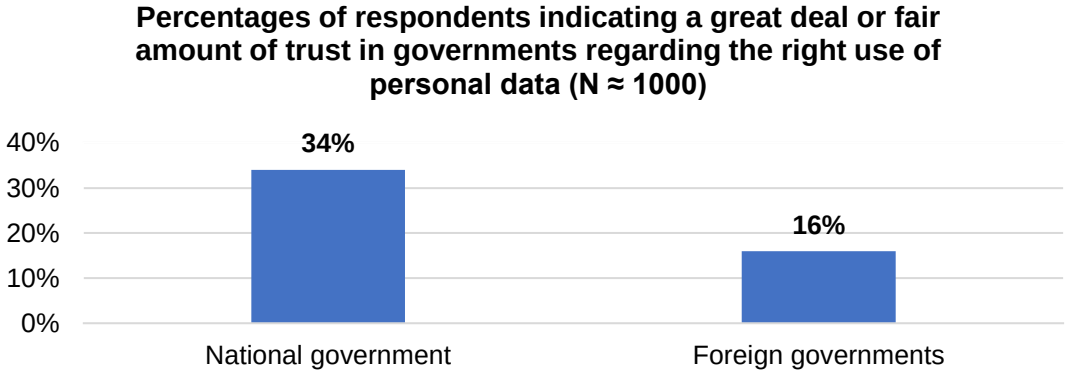

Fig. 10. Percentages of respondents indicating a great deal or fair amount of trust in governments regarding the right use of personal data (Ipsos 2019, p. 20).

Moreover, national, and foreign governments seem to contribute to Americans' distrust of the Internet in general. 86% of Americans indicate that national governments contribute to distrust of the Internet, and 84% name foreign governments as contributors to distrust of the Internet (Fig. 21) (cf. CIGI-Ipsos 2019a, p. 117, 2019c, p. 20). However, reasons of how governments contribute to distrust remain unclear. Only 24 (or 15% regarding foreign governments) of Americans indicate that governmental control of the internet contributes to distrust of the Internet (cf. CIGI-Ipsos 2019a, p. 119, 2019c, p. 22).

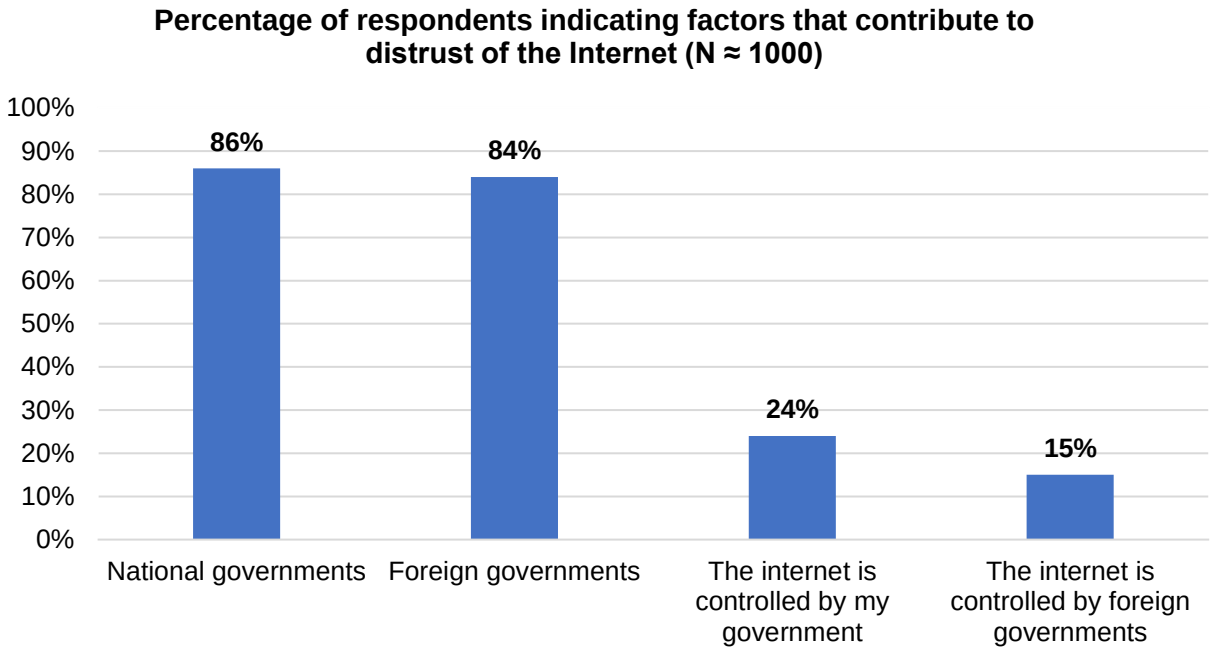

Fig. 11. Percentages of respondents indicating factors that contribute to distrust of the Internet (CIGI-Ipsos 2019a, 117, 119, 2019c, 20, 22).

2. Attitudes Towards Companies

Trust in companies' efforts to protect personal data is similarly low as Americans' trust in governments. 69% of 4272 Americans deny that companies use Internet users' information in ways they feel comfortable with, 57% are not at all or not too confident that companies adhere to their own privacy policies, and 65% doubt that companies will notify them if their personal data has been misused or compromised (cf. Auxier et al. 2019, pp. 9–10). Moreover, majorities believe that companies will not publicly admit mistakes in data use (79%) (cf. Auxier et al. 2019, p. 4).

However, Americans' confidence in companies' abilities to protect their data is still higher than their trust in governments. One in two respondents agree that companies put enough effort in data protection, whilst only 36% express their confidence in the domestic government (cf. CIGI-Ipsos 2019b, p. 45, 2019c, p. 283) (Fig. 22).

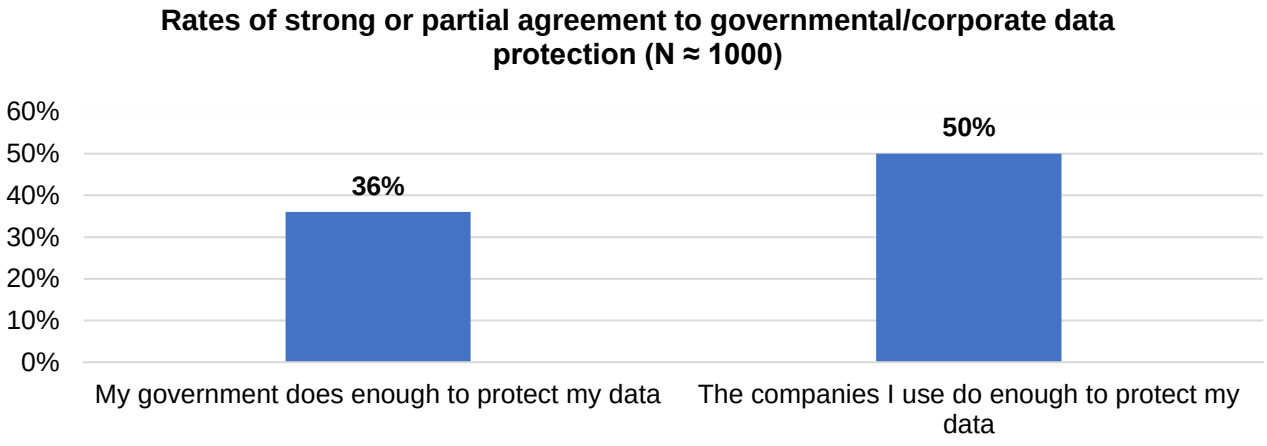

Fig. 12. Percentage of respondents that strongly or somewhat agree to governmental and corporate efforts for data protection (cf. CIGI-Ipsos 2019b, p. 45, 2019c, p. 283).

The American public's distrust of governments to hold companies accountable for misusing users' data (75%) further adds to the argument that trust in corporate data protection is a bit higher than trust in governments (cf. Auxier et al. 2019, p. 9), which again relates to Americans' distrust of governmental data protection. A majority of Americans (75% of 2140 survey respondents) asks for more regulations that companies should have to follow to protect personal data.

Moreover, Americans' confidence does not only vary between companies and governments, but also between several industries when it comes to data protection. Fig. 23 illustrates that Americans especially trust healthcare providers, financial services companies, and shipping/delivery companies to use their personal data correctly.

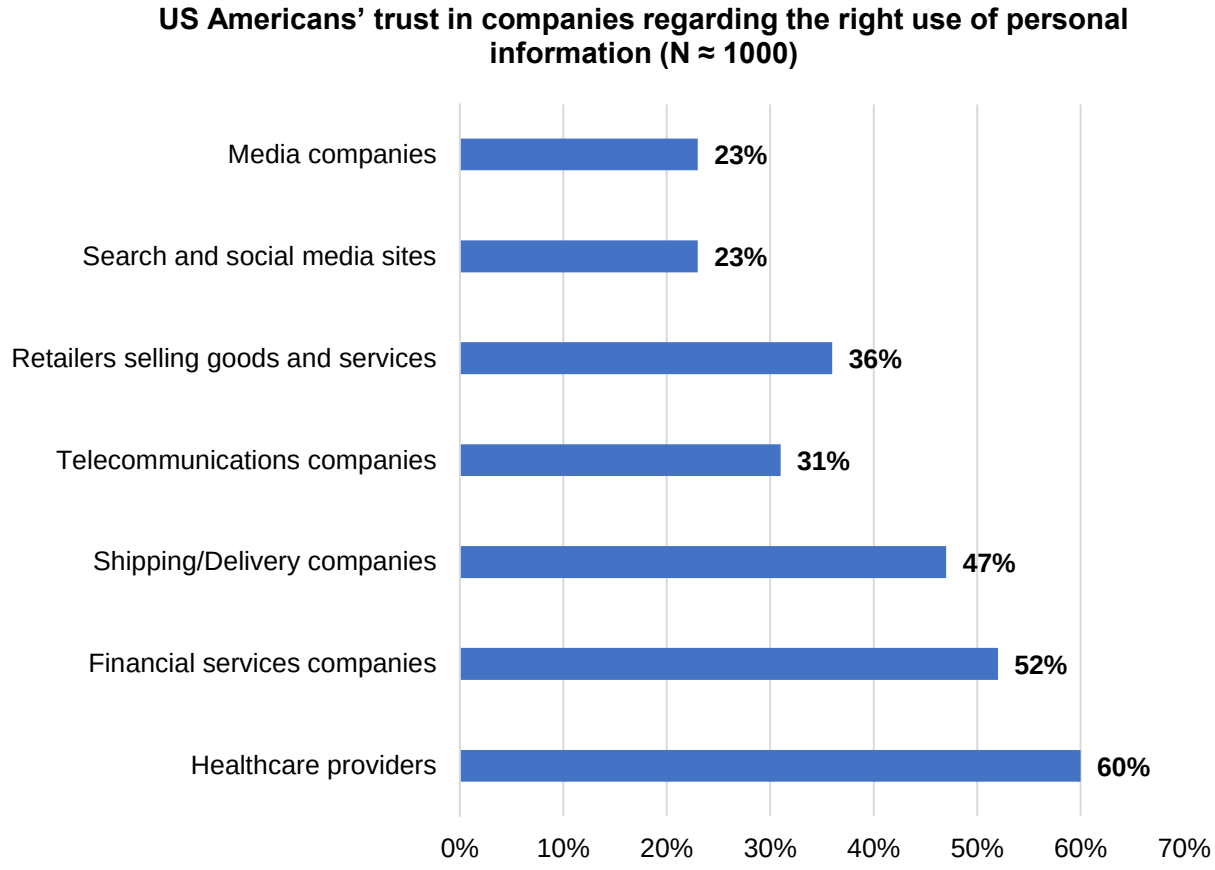

Fig. 13. Americans' trust in institutions regarding the right use of personal information (cf. Ipsos 2019, p. 20).

Conversely, Americans are less likely to express their trust in telecommunications companies, retailers, search and social media sites, and media companies (cf. Ipsos 2019, p. 20). High distrust ratings in social media (87%), search engines (74%), Internet service providers (70%), e-commerce platforms (59%), and online and mobile banking platforms (57%) additionally mirror that such companies are not considered as trustworthy (Fig. 24).

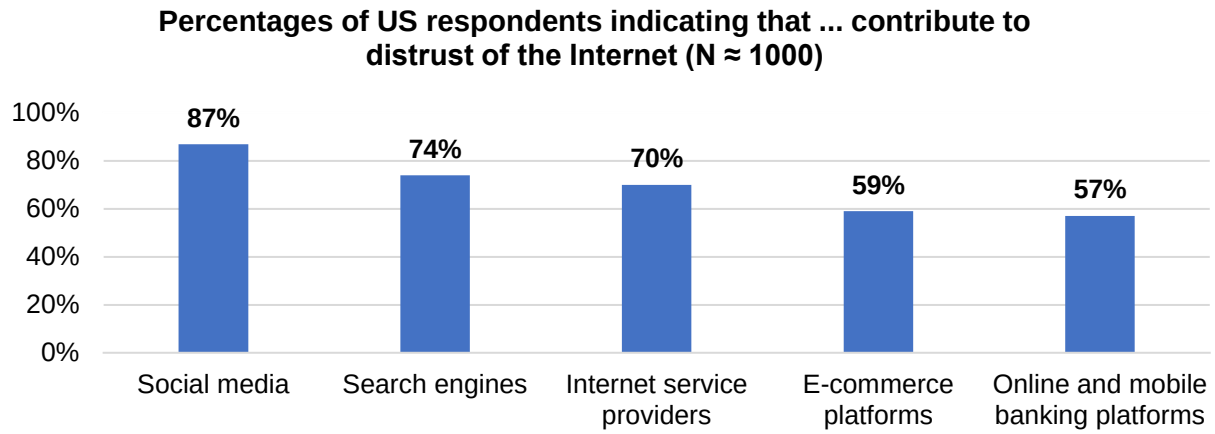

Fig. 14. Percentages of US respondents indicating that the mentioned media, platforms, or industries contribute to distrust of the Internet (cf. CIGI-Ipsos 2019c, p. 20).

Americans also seem to express more trust in companies that use their data for specific purposes. Whilst more adults (57% of 4272 respondents) are more comfortable with companies using their personal data to help improve fraud prevention systems, less are comfortable with data sharing for scientific research (64% indicate that they would be uncomfortable). Overall, younger adults (18-49 years) are more comfortable with the use of personal data for the aforementioned reasons than adults older than 50 (cf. Auxier et al. 2019, p. 40).

X. Communication on Data Use

[This] parameter […] relates to the importance [US respondents] attribute to communication on how their personal data are used.[11]

Companies that communicate what they will do with collected information are more likely to receive consumers' confidence. 69% of approximately 1000 surveyed respondents indicate that they are much or somewhat more confident in sharing their data with companies that inform them about what they will do with the information, and 66% indicate their confidence with companies that promise not to share or sell the data to other parties (Ipsos 2019, p. 14) (Fig. 25). Furthermore 43% indicate that they would be willing to give a company or governmental organization access to their data if they are clearly informed about the risks they are exposed to (cf. Ipsos 2019, p. 17).

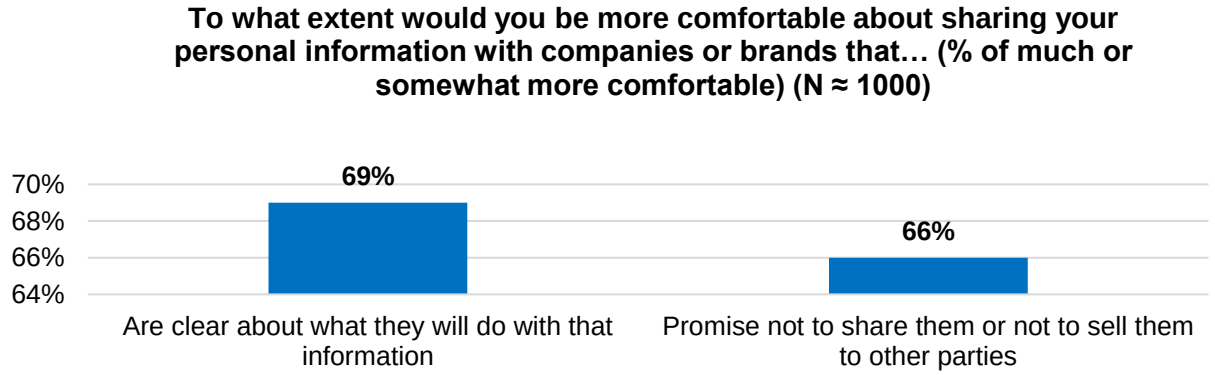

Fig. 15. Communication on data use (cf. Ipsos 2019 p. 14).

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

XI. Key Findings

This report gives an overview of US Americans' assessments on issues of informational privacy, data protection, and data control pertaining to personal data disclosure. In what follows, the main insights are summarized.

1. Digital Competitiveness

Regarding digital competitiveness, the US has led the IMD Digital Competitiveness Ranking for four years consecutively since 2018. In the latest ranking in 2021, the US has proven strengths in issuing venture capital for innovation, in fostering research, and in encouraging the public's participation in online transactions. However, the US appears less strong in motivating young people to studying natural sciences or engineering.

2. General Value of Informational Privacy

Results indicate that a majority of Americans (67.7%) accepts governmental surveillance in public areas as well as corporate workplace monitoring (88%). However, few promote governmental email monitoring (22.9%) or secret data collection without people knowing about it (28.1%). Regarding corporate data collection, most Americans agree that consumers should either receive compensation in return for their data (61%) or should be able to refuse that companies can make use of collected data (75%). Only few respondents indicate that they do not bother about corporate data collection (23%).

3. The Degree of Privacy of Data

As for the degree of privacy of data, mean values indicate that American social media users are most sensitive about data that relates to their sexual behavior, personal weaknesses, and savings.

4. Benefits Associated with Data Disclosure

Overall, most Americans associate less benefits than risks with data disclosure to governments or companies. As benefits, they indicate saving money (28%) and time (34%), an increased customer experience, because it helps providing relevant products, services, and information (44%), altruistic motives, e.g., improving students' educational performance (49%) or for security reasons, e.g., if data disclosure helps to prevent terrorist attacks (49%).

The contexts in which data use is accepted vary with age. Younger survey respondents (aged 18-29) are for example more likely to accept data collection on social media for monitoring signs of depression to advertise treatment opportunities (42%), or through fitness apps that share medical data with researchers (52%). Older survey respondents (older than 64) show more acceptance of data collection if it helps solving crimes (58%) or preventing terrorist attacks (54%). Ultimately, a large amount of Americans would be more comfortable with data disclosure if they received compensation in return (66%).

5. Privacy Concerns and Risks

a. Data Security

Concerns about data security have increased since 2015, especially among people who are following privacy news closely (74%). Moreover, a large amount of Americans have experienced data breaches in general (61%), and rich people (75%), respondents with college degrees (78%), and respondents older than 50 (73%) indicate the most pronounced concerns. When it comes to specific types of data breaches, fraudulent charges on credit cards appear to be the most noted (indicated by 41% of US respondents). Fewer respondents seem to have received notices on

compromised personal information (35%) or have been affected by unauthorized credit transactions (14%). Very few further indicate that tax refunds had been taken out in their name (6%) or that social media accounts were taken over without permission (13%). Regarding data security abroad, a lot of Americans seem to prefer storing their online data and personal information on secure servers in the US (73%) instead of transferring it to secure servers outside the country (24%). Only few indicate their indifference towards data that leaves the country, be it personal data (29%), corporate data (31%), or governments' data (27%).

b. Data Control

A large consensus on data control among US respondents seems to rely on the belief that data tracking cannot be prevented (60%). At the same time, concerns about data control vary with the type of data shared. Concerns on what social media sites know about consumers are especially high (85%), followed by concerns on what advertisers (84%), and companies where people buy things from (80%) know about consumers. Furthermore, Americans perceive no or little control over who can access search terms they use online (89%), who can track websites consumers visit (85%), who can retrace purchases (88%), or data on physical location (82%), posts, or other activities on social media (85%).

Moreover, concerns about data control seems to vary between ethnic groups. Whilst White Americans tend to worry more about corporate data collection (50% of White vs. 66% of Hispanic and 69% of Black Americans), Black and Hispanic Americans seem to be more concerned about governmental data tracking (43% of White vs. 56% of Hispanic and 60% of Black Americans).

Regarding consequences of privacy concerns in terms of distrusting the Internet, polls indicate that most Americans decide to simply disclose less personal information online (52%) or take greater care to secure their devices (43%). Few indicate using the Internet more selectively (38%) or self-censoring what they say online (35%), and very few make fewer purchases (18%) as a consequence of distrusting the Internet.

6. Data Protection Literacy

Americans' awareness and knowledge of data protection is low (33%). Americans tend to overestimate their ability to protect their privacy (60% indicate high confidence in their ability to protect their personal data), and few read privacy policies all the way through before they opt into companies' policy statements (9%). Regarding the application of privacy settings, women (69%) and younger people (77%) indicate more use of privacy settings than men (61%) and people older than 64 (32%). Moreover, respondents with higher levels of education and higher income seem to be more prone to use privacy settings. Whilst 72% of college graduates indicate using privacy settings, only 49% of people without a college degree indicate the same. In a similar vein, people with lower income (57%) use less privacy settings than people with higher income (67%). Interestingly, foreign-born Hispanics are the ones least likely to indicate high confidence in their data protection skills (29%) whereas they are the ones most likely to asking for more education on privacy-related topics (Madden 2017a, p. 92).

Overall, it becomes evident that data protection literacy rises with income and level of education. In addition, younger respondents, women, and people from urban areas are more likely to apply privacy protection than older ones, men, and residents of rural areas. Ultimately, data protection literacy varies with ethnic backgrounds and is most present in white American populations, less in Black communities, and least in foreign-born Hispanic groups of respondents.

7. Attitudes Towards Data Receiver

a. Attitudes Towards Governments

Only 37% of respondents from the USA think that most people can be trusted. Confidence in how governments use personal data is low and mirrors Americans' general distrust towards governments. Trust in foreign governments (16%) is even lower than trust in national governments (34%). Vice versa, majorities of Americans perceive that national (86%) and foreign governments (84%) contribute to their general distrust of the Internet. In addition, 75% of Americans call for more governmental regulation on data privacy, with Democrats (81%) being especially keen on changing existing privacy laws.

b. Attitudes Towards Companies

Trust in companies to protect user data is also low, yet it is slightly higher than trust in governments. Whilst 50% of Americans believe that companies do enough for data protection, only 36% of respondents indicate the same for governments. Moreover, trust varies between industries and Americans seem to rather trust healthcare providers (60%), financial services companies (52%), and shipping/delivery companies (47%) to use their data correctly. In comparison, retailers (36%), telecommunications companies (31%), search and social media sites (23%), and media companies (23%) are considered as less trustworthy. This could hint to more skepticism towards platform business models compared to more traditional business models, e.g., in the healthcare sector.

In addition, the purpose for which companies use data also affects respondents' attitudes. More Americans consider the use of data for customers' security as more desirable than the use of data for scientific research. Especially younger respondents are more comfortable with companies using customers' data than older Americans.

8. Communication on Data Use

Confidence in companies is highest when companies clearly communicate what they will do with user data. A high amount of Americans indicate that they would be more comfortable about sharing their data with companies that communicate clearly about what they will do with the information (69%). Slightly less indicate their confidence towards sharing data with companies that promise not to share or sell data to other parties (66%).

XII. References

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (last access: 12/15/2021).

Black Lives Matter (2021, July 8). Home - Black Lives Matter. https://blacklivesmatter.com/ (last access: 12/15/2021).

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).

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. https://www.worldvaluessurvey.org/WVSEVSjoint2017.jsp (last access: 12/15/2021).

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

Globe. (2020). An Overview of the 2004 Study: Understanding the Relationship Between National Culture, Societal Effectiveness and Desirable Leadership Attributes. https://globeproject.com/study_2004_2007#theory (last access: 12/15/2021).

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 [Ipsos-World Economic Forum Tracking Study on Consumer Acceptance of Information Technology]. Ipsos; World Economic Forum. https://www.ipsos.com/sites/default/files/ct/news/documents/2019-01/ipsos-wef_-_global_consumer_views_on_data_privacy_-_2019-01-25-final.pptx_lecture_seule_0.pdf?mod=article_inline (last access: 12/15/2021).

Jourard, S. M., Lasakow, P. (1958). Some Factors in Self-Disclosure. Journal of Abnormal Psychology, 56(1), 91–98. https://doi.org/10.1037/h0043357 (last access: 12/15/2021).

Madden, M. (2015). Privacy and Security Experiences of Low-Socioeconomic Status Populations. Data & Society Research Institute. https://datasociety.net/library/privacy-security-and-digital-inequality/ (last access: 12/15/2021).

Madden, M. (2017a). Privacy, Security, and Digital Inequality. Data & Society. https://datasociety.net/library/privacy-security-and-digital-inequality/ (last access: 12/15/2021).

Madden, M. (2017b). Privacy, Security, and Digital Inequality: How Technology Experiences and Resources Vary by Socioeconomic Status, Race, and Ethnicity. Survey Data Files. Final Questionnaire. Data & Society. https://datasociety.net/library/privacy-security-and-digital-inequality/ (last access: 3/12/2021).

Olmstead, K., & Smith, A. (2017). Americans and Cyber-Security: Many Americans Do Not Trust Modern Institutions to Protect their Personal Data – Even as they Frequently Neglect Cybersecurity Best Practices in their Own Personal Lives. Pew Research Center. https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/ (last access: 12/15/2021).

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

Trepte, S., & Masur, P. (2016). Cultural Differences in Social Media Use, Privacy, and Self-Disclosure. http://opus.uni-hohenheim.de/volltexte/2016/1218/pdf/Trepte_Masur_ResearchReport.pdf (last access: 12/15/2021).

Vogels, E., & Anderson, M. (2019). Americans and Digital Knowledge. Pew Research Center. https://www.pewresearch.org/internet/2019/10/09/americans-and-digital-knowledge/(last access: 12/15/2021).

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: 03/04/2022).

Appendix 1. List of included studies and study details

Study	Overview	Sample size per country	Demographics and unweighted sample size per group
Americans and Cyber Security (Olmstead and Smith 2017)	The survey examines Americans' attitudes about cyber security policy, their experiences with cyber security, and individuals' capability to manage their own digital security with a focus on password management.	N = 1040	All Adults 18+: 1040 18-29: 170 30-49: 283 30-49: 283 50-64: 325 65+: 234 Men: 509 Women: 531 High school (HS) or less: 303 Some college: 265 Bachelor's degree or more: 462
Americans and Digital Knowledge (Vogels and Anderson 2019)	The study evaluates results from a digital knowledge quiz that was conducted online to check what U.S. adults know about, e.g., cybersecurity and privacy questions.	N = 4272	Age group: 18-29: 671 30-49: 1314 50-64: 1308 65+: 977 HS or less: 1483 Some college: 1182 College+: 1600
Americans and Privacy: Concerned, Confused and Feeling Lack of Control over their Personal Information (Auxier et al. 2019)	The study analyses Americans' privacy concerns, e.g., the growing distrust of personal data security, data collection, as well as daily tracking issues in the US.	N = 4272	Age group: 18-29: 671 30-49: 1314 50-64: 1308 65+: 977 Men: 1875 Women: 2397 HS or less: 1483 Some college: 1182 College+: 1600 Income: Less than 30000: 1107 $30,000 - $47,999: 1469 $75,000+: 1496

Study	Overview	Sample size per country	Demographics and unweighted sample size per group
			White, Non-Hispanic: 2887 Black, Non-Hispanic: 445 Hispanic: 611 (Lean) Republicans: 1823 (Lean) Democrats: 2296
CIGI-Ipsos Global Survey on Internet Security and Trust Part I/II (CIGI-Ipsos 2019a)	The survey examines how privacy concerns have increased around the world and how distrust of the Internet affects global citizens in their use of the Internet. Moreover, the survey evaluates reasons for increasing privacy concerns and factors that contribute to distrust of the Internet.	N ≈[12] 1000	Age: 18-64
CIGI-Ipsos Global Survey Internet Security & Trust Part 6: Cross-Border Data Flows (CIGI-Ipsos 2019b, 2019c)	The survey observes awareness of data protection and privacy rules, attitudes towards cross-border data flows, secure data storage, governmental and corporate ability to protect data.	N ≈[13] 1000	Age: 18-64
Global Citizens and Data Privacy Study, Ipsos & World Economic Forum (Ipsos 2019)	The survey tracks public understanding as well as actual acceptance of new technologies around the globe.	N ≈[14] 1000	Age: 18-64
Cultural Differences in Social Media Use, Privacy, and Self-Disclosure (Trepte & Masur 2016)	The report presents results on social media use, self-disclosure, privacy perceptions and attitudes, and privacy behavior in online environments from a cross-cultural survey.	N = 555	Average age: 20 Men 44.9% Women 55.1% High school: 0.2% 2 year college: 45.2% Bachelor: 19.1% Master: 34.7% PHD: 0.9%

[12] Indicates an approximate amount of survey respondents. Survey institutes state that the surveyed individuals were "weighted to match the population in each economy surveyed. The precision of Ipsos online polls is calculated using a credibility interval. In this case, a poll of 1000 is accurate to +/- 3.5 %age points" CIGI-Ipsos (2019a, p. 4).

[13] Indicates an approximate amount of survey respondents. Survey institutes state that the surveyed individuals were "weighted to match the population in each economy surveyed. The precision of Ipsos online polls is calculated using a credibility interval. In this case, a poll of 1000 is accurate to +/- 3.5 %age points" (CIGI-Ipsos 2019b, p. 4).

[14] Indicates an approximate amount of survey respondents. The survey institute state that "precision of Ipsos online polls is calculated using a credibility interval with a poll of 1000 accurate to +/- 3.5 %age points and of 500 accurate to +/- 5.0 %age points" (Ipsos 2019, p. 21).

Study	Overview	Sample size per country	Demographics and unweighted sample size per group
World Values Survey (EVS/WVS 2021)	The cooperation between the European and the World Values Survey investigates values that are most important to people from different national backgrounds, including values that relate to attitudes towards data disclosure.	N = 2596	Individuals aged 18+ of any nationality, citizenship or language, residing in the US within private households for the past 6 months prior to the date of beginning of fieldwork