Blockchain Research Lab

Digital Identity and Personal Data in 2020: Citizens' Opinions and Motives

Results of a representative online survey in Germany

Report No. 6

November 4th, 2020

Executive Summary

Based on a representative survey among 1,000 German adult internet users, this report offers insights about the motivational factors for using digital identity solutions and risk perceptions towards the sharing and provision of personal data online as well as the trust placed in companies and institutions handling personal data.

Citizens see “trust” and “actual benefits” of digital identity solutions as the most important motives, whereas “social motives” are subordinate. The highest risk associated with sharing personal data online is perceived to be its undetected usage without consent. Most personal data are provided for authentication while logging into specific online systems. The most trusted organizations handling personal data are friends and family, followed by public authorities and government institutions. The overall level of trust with regard to personal data handling is rather low, whereas the lowest trust is placed in companies' unknown to them and internet companies.

About us

The non-profit organization Blockchain Research Lab is dedicated to independent science and research on blockchain technology and to publishing the results for the benefit of society. The Blockchain Research Lab works on the identification of the socio-economic implications of blockchain technology. This includes the identification and analysis of use cases and their social potentials and risks.

The project on which this report is based was funded by the Federal Ministry of Economics and Energy (BMWi) under the funding code 01MN200006E. The author is responsible for the content of this publication.

About STEREO

The results presented in this survey were identified within the scope of the project *STEREO (Sichere Digitale Identität für kommunale Mobilitätsservices)*, which is part of the innovation showcase programme *Secure Digital Identities* in Germany. The project was funded by the *Federal Ministry for Economic Affairs and Energy (BMWi)* under funding code (01MN20006E) and focuses on the topic of self-sovereign identities (SSIs). It aims at creating and linking secure digital identities of individuals and objects for municipal mobility services. The project consortium was initiated by *Christoph Kroschke GmbH*. Other partners in the consortium include *Chainstep GmbH*, *Osborne Clarke*, *HAW Hamburg*. Further information regarding the project and the consortium can be found at stereo-hamburg.de.

Introduction

Data security is an urgent topic, especially in the realm of personal data on the internet. On the individual level, protecting personal data can be challenging, as many online services can only be accessed through the provision of data to service providers. Online data protection is between the poles of security on the one side and convenience on the other. Individuals are relying on the security measures taken by service providers to protect their data, whereas service providers aim to design their services with as little inconvenience as possible for their users for increasing conversions and optimizing user experiences. A preliminary state from this field of tension is characterized by siloed solutions for federated identity systems and the prerequisite of sign-ups and logins for accessing online services, requiring end users to repeatedly enter their personal data. Alongside technical evolvement of security measures, this current state highlights the necessity for policy and economy to continuously gain insights into the views, motives and preferences of end users. For service providers, governmental institutions and citizens it is equally important to understand which challenges end users face when dealing with identity data online, which features are demanded, and which measures will be accepted. This report presents insights on end users' perceptions on digital identity and personal data on the internet. The results contribute to the scientific, technological and regulatory discourse of the topic and can be incorporated into the development of secure identity systems.

Methodology and sample description

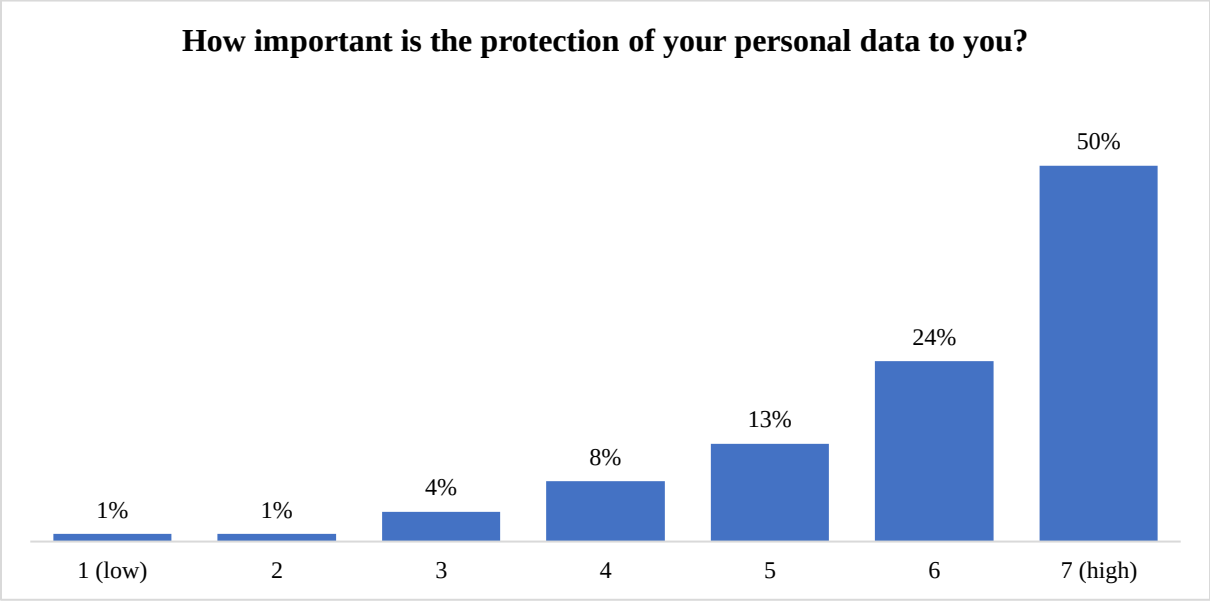
This report builds on the data of 1,000 German internet users, i.e., people who were online at least once in the last quarter year and is representative of the German internet-using population in terms of age and gender. To be more precise, the sample comprises 49% males and 51% females, whereas each sex-related subsample is representative based on five different age groups: 18-24, 25-39, 40-59, 60-64 and 65 years and above. The participants responded to an online questionnaire, which was conducted in August 2020 by a panel provider that maintains a panel of more than 150,000 individuals in Germany for online surveys. The survey was conducted during the COVID-19 pandemic, which may have an influence on individual's answers. To ensure high data quality, participants who sped through the survey, i.e., answered

too quickly for their answers to carry much meaning, were manually dropped. The panelists were invited by e-mail, while initially no indication was given as to the topic of the survey to exclude any bias from, e.g., self-selection. Monetary rewards for participation were offered. The questions presented in this report were asked in German and have been translated.

Generally, any recruitment of survey participants is likely subject to a certain bias. For example, conducting a telephone survey requires respondents not only to own a phone but also to accept an unknown caller and to have the time and interest to then answer the questions. This is certainly more likely for some parts of the population than for others. Similarly, our sample only comprises those who were willing to join a panel. In consequence, it is likely that certain subgroups of the population are overrepresented, for example people who are affine to the internet, have time to answer surveys and are comfortable providing personal details online. While our sample is approximately representative based on age and gender, we cannot claim representativeness of the population in all regards (e.g., education status, job etc.).

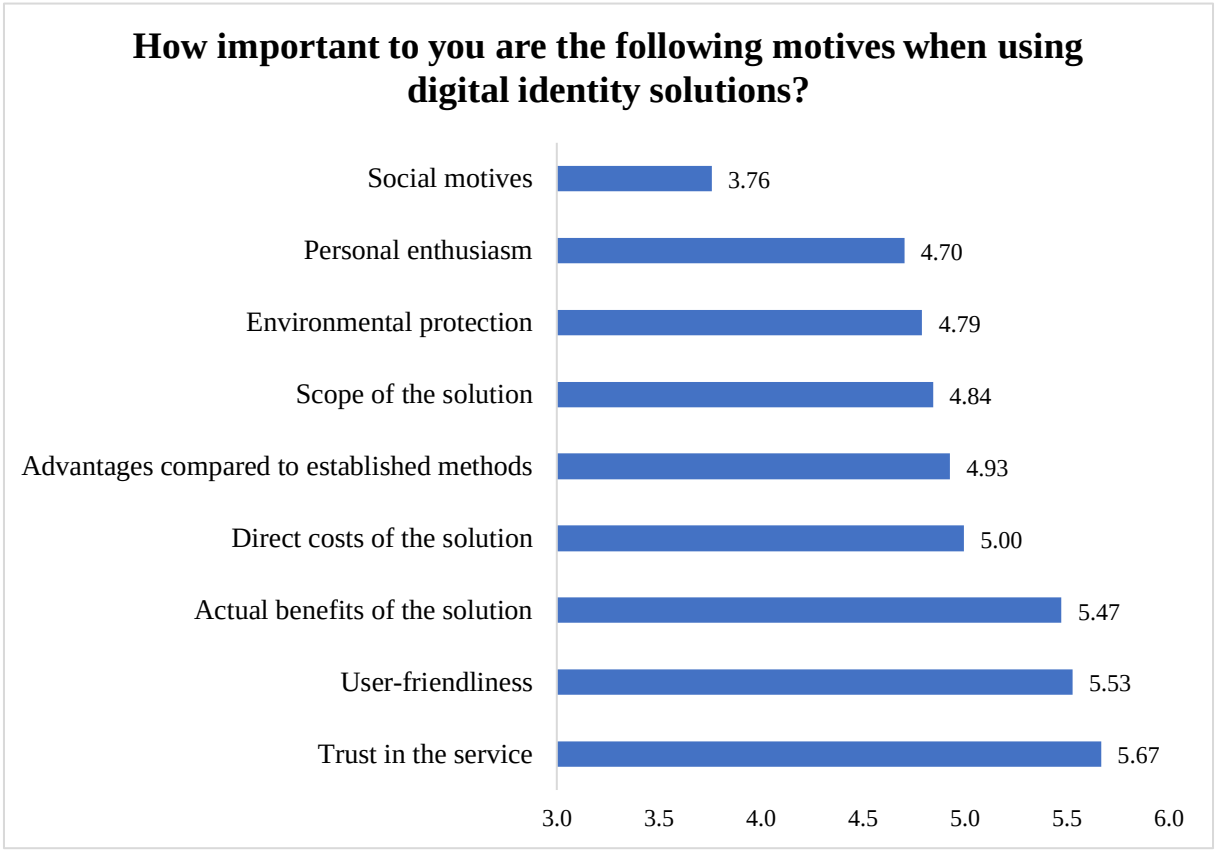
Data protection

With regard to data protection, respondents were asked to indicate how important the protection of their personal data is to them individually. They were able to rate on a scale from 1 (not important) to 7 (very important). As Germany is generally perceived as a state in which data protection is an important issue, it is not surprising that half of the respondents indicated the highest possible level of importance. The relatively high average rating of 6 underlines the importance of the topic among our sample. Women we found to value data protection slightly more important than men.



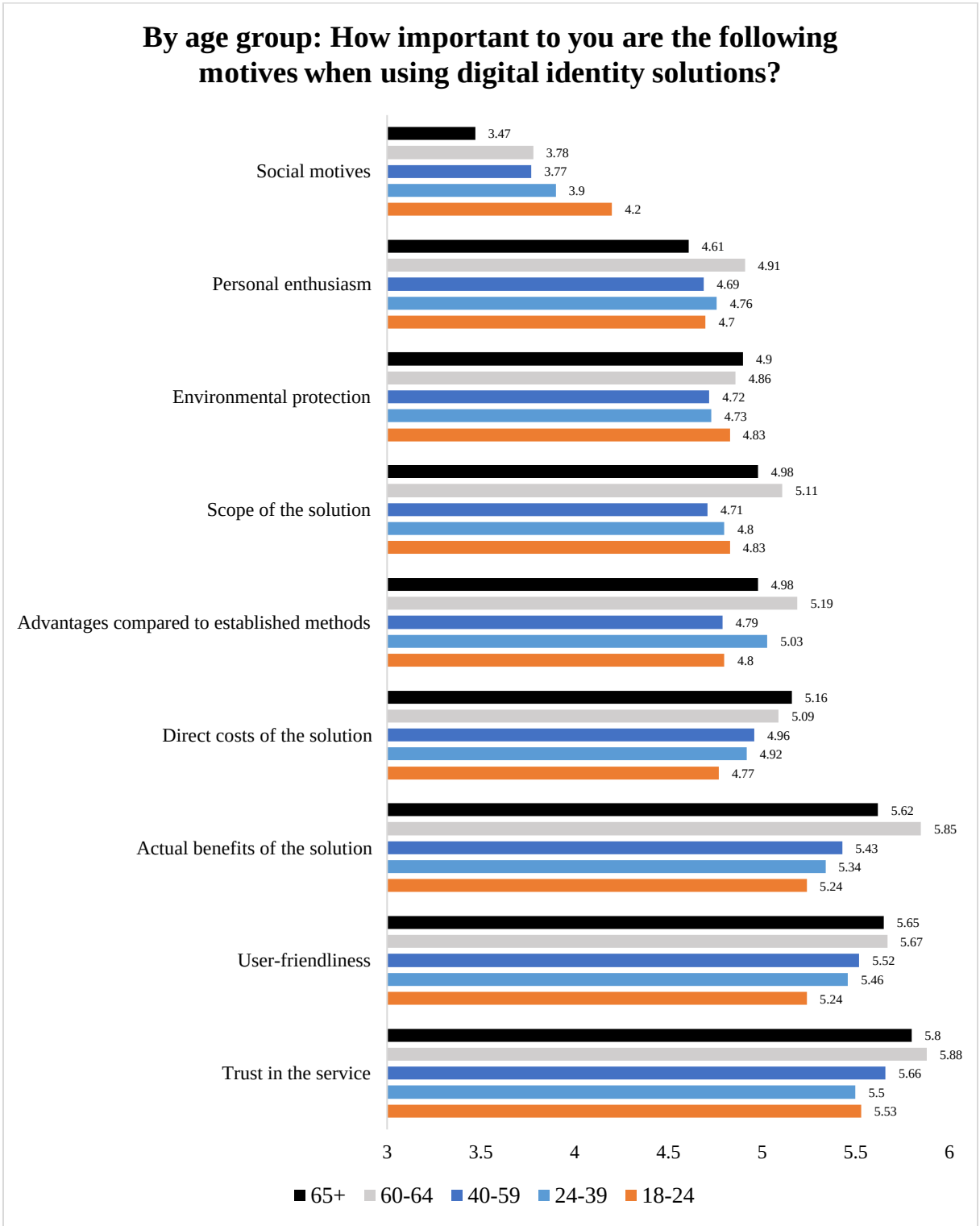
Digital identity solutions

When surfing the internet and accessing online services, every user leaves a trace. May it be browsing history and settings through cookies or data transmitted for login authentications, every activity requires data packages of different kinds to be transmitted across the internet with varying extent of personal data. Given the variety of services which in one or another way authenticate identities, such as login-buttons (e.g., Login with Google) or user name and password, citizens were asked about their most important motives for using different solutions. Nine pre-selected motives were presented and respondents indicated their considerations on a scale of 1 (not important) to 7 (very important), i.e., the score 4 represents a neutral midpoint. The results are visualized in the following figure.



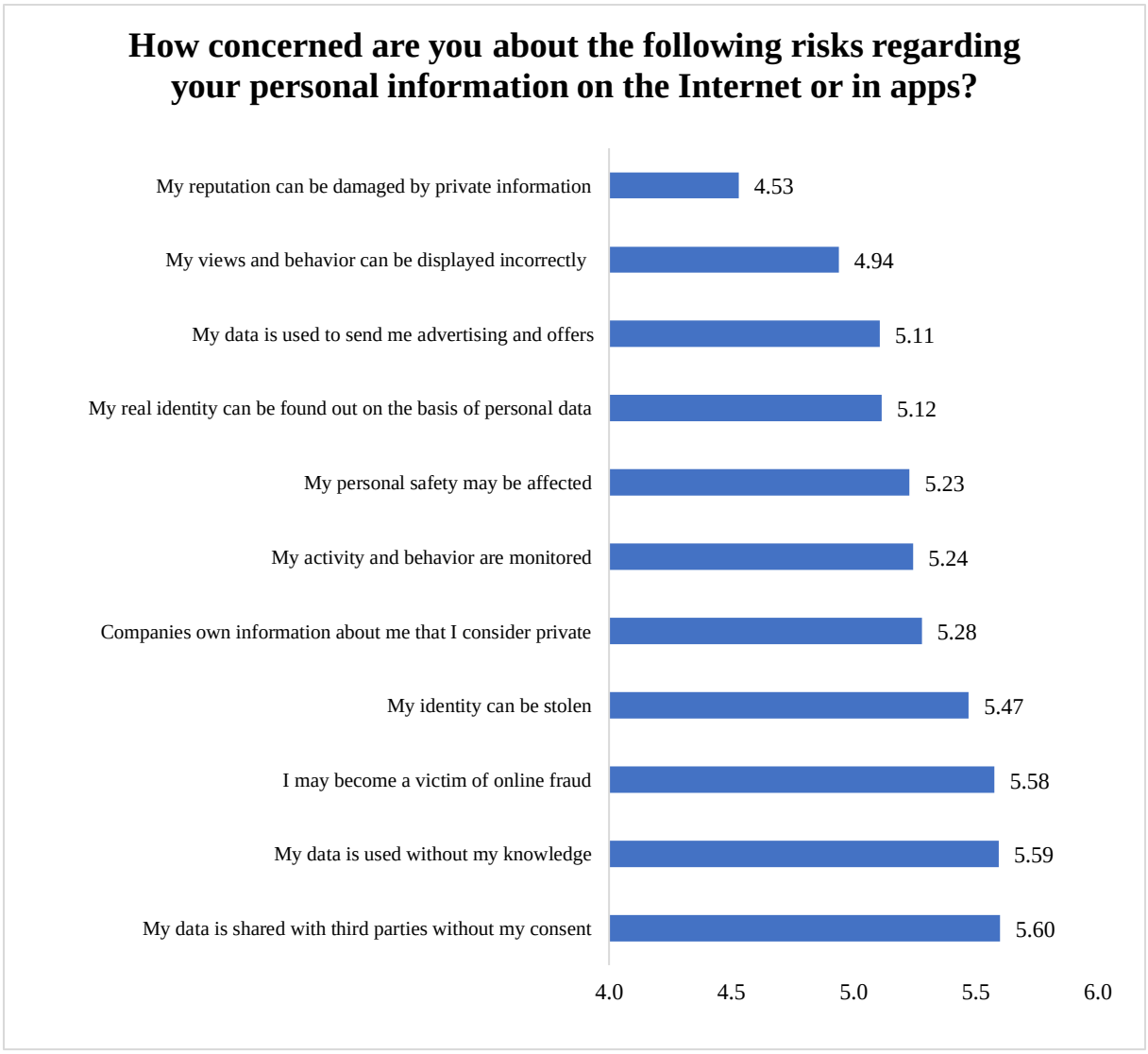
The majority of motives are valued above the "neutral" scale point. "Trust in the service" is considered most important by the respondents, followed by "user-friendliness" and "actual benefits of the solution". The chart shows that "social motives" is considered the least relevant motivation for using specific identity services. It can be concluded that people first and foremost have the benefit of identity solutions in mind. Higher or indirect motives such as enthusiasm, environment or social issues are secondary. The analysis of gender-specific differences showed that women rated the different motives slightly higher on average, except for the two motives "Scope of the solution" (i.e., the ability of a system to work with other systems or the number of services offered) and "Direct costs" of the solution, e.g., the fee for an app.

Differentiating the results by age groups (see Figure below), the survey revealed that older individuals specifically find “actual benefits” of a solution most relevant. In contrast, “social motives” become less relevant with higher age, which confirms current tendencies that sustainability is a high priority for the younger generation. Younger respondents see the direct costs of a solution as comparatively less relevant than older people. Similarly, younger respondents consistently rank each motive less important, i.e., across the high-leveled choices.



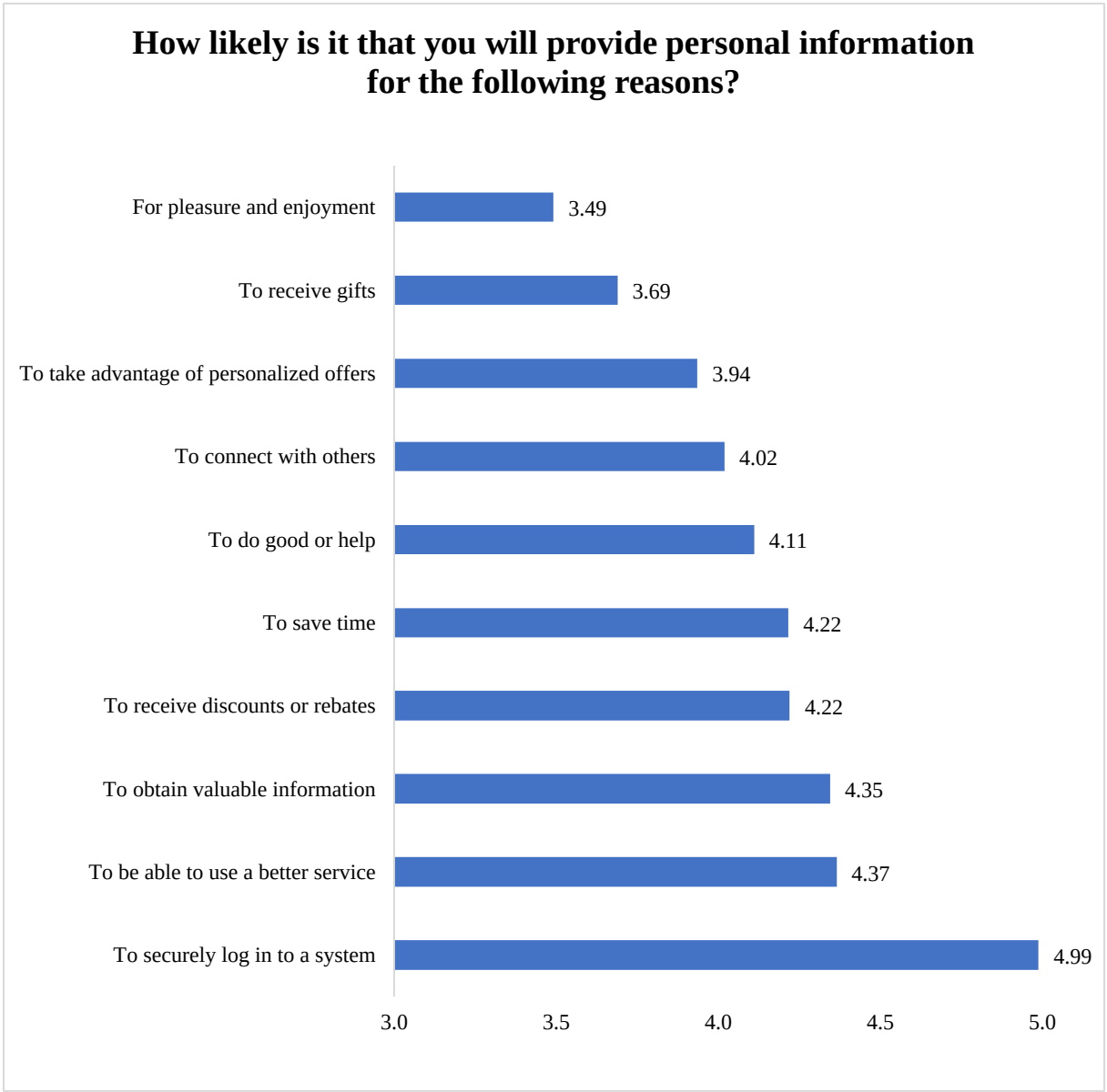
Personal information on the internet

Survey participants were asked to evaluate which of eleven pre-selected risks associated with personal data online concerned them the most on a scale of 1 (not very concerned) to 7 (very concerned). None of the risks presented can be regarded irrelevant, as all levels exceed the scale's neutral point 4. The highest rated risk is that personal data could be used by third parties without consent of the originator. A very similar risk of using data without the knowledge of the individual was also rated very high. The third highest ranking is the risk of becoming a victim of online fraud. The risk of damage to the individual's reputation rates comparatively lower than all other risks. This is in line with the "Digital Government Barometer 2019" survey[1], in which the authors find that 23% of the 999 respondents in Germany were very concerned that data could fall into the wrong hands or used improperly (20%). Security concerns were the most frequently cited reasons as well.



[1] https://www.soprasteria.de/newsroom/publikationen/digital-government-barometer-2019

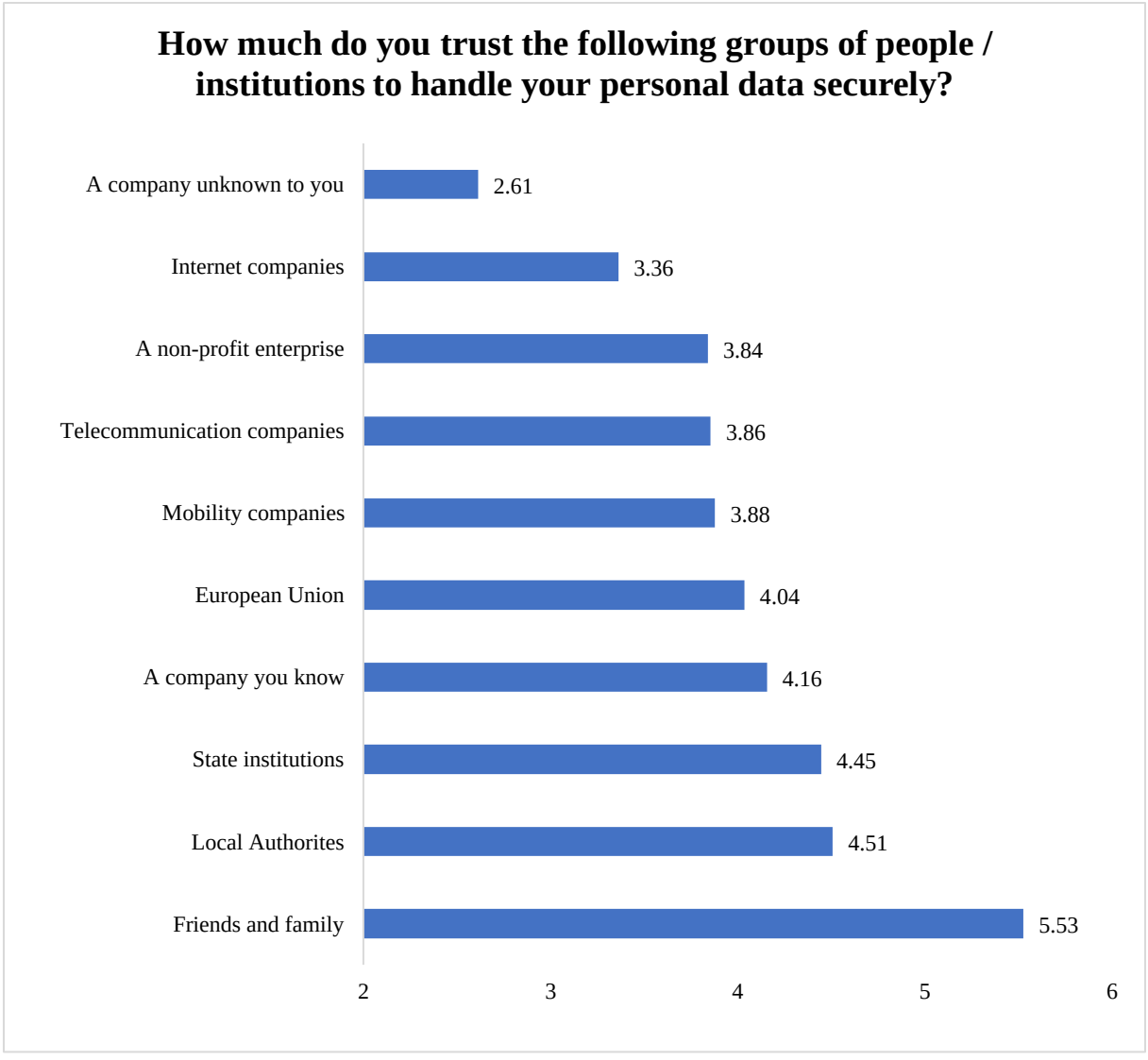
The following question was focused on assessing the reasons why respondents provide personal data online. The respondents were asked how likely they estimate the chance for providing personal information for specific pre-selected reasons or benefits. Again, they ranked the likeliness of providing information on a scale from 1 to 7, whereas 1 represents lowest likeliness and 7 highest. The most “important” reason for transmitting personal data is to securely access a system online - access that would otherwise probably not be possible. Future research might dig into the related question, which systems respondents log into the most, and which data they are willing to share for different service categories.



Other important reasons include the use of better services, such as additional features or access to valuable information. For example, people could have an interest to log in to access news sites or messaging apps. The motive "for pleasure and enjoyment" clearly ranked lowest. This may be an indication that individuals expect a certain kind value for the commission of personal information.

Trust in third-parties to handle personal data

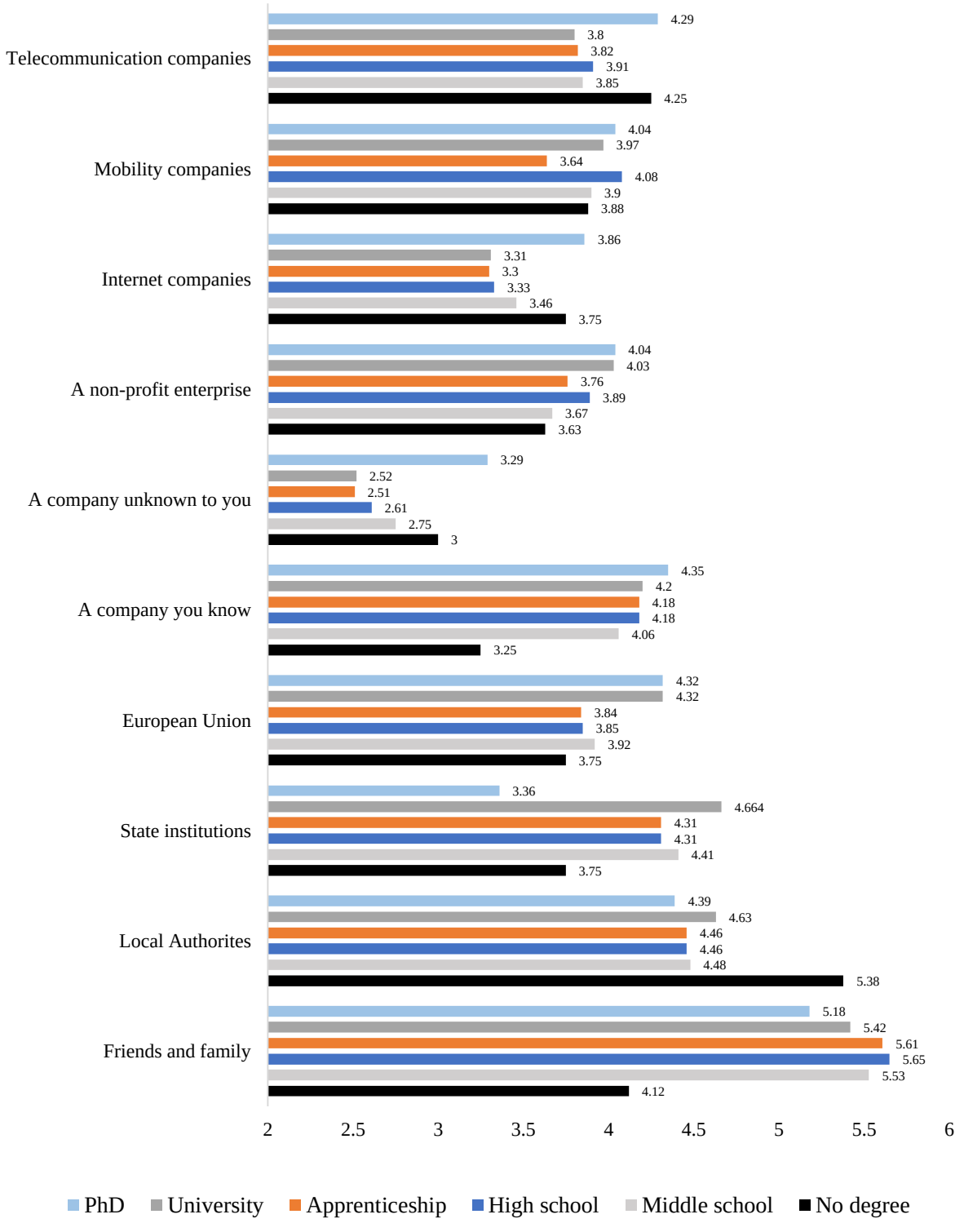
Individuals were asked how much they trust the groups or institutions listed in the following figure to handle their personal data securely. They could choose from 1 (very low) to 7 (very high). Looking at the scale interval, it is revealed that the overall trust perceptions are comparably low. Half of the possible choices are below the center of 4, the other half is above. At the same time the highest and lowest rank can be identified very clearly. The highest trust is - less astonishing - placed in friends and family followed by local and state institutions. The European Union, with a value of 4.04, which is only just above the midpoint, is only much less trusted than national authorities. The lowest value is given to unknown companies, followed by internet companies and - surprisingly - non-profit enterprises. This indicates that the population's trust in state institutions is higher than in private companies and is in line with the results by Sopra Steria's "Digital Government Barometer 2019"[2] and the "eGovernment Monitor 2019" of the Initiative D21 and fortriss[3].



[2] https://www.soprasteria.de/newsroom/publikationen/digital-government-barometer-2019
[3] https://initiatived21.de/publikationen/egovernment-monitor-2019/

When looking at subsamples based on educational levels, it can be seen that trust in authorities decreases with educational level, while it increases for the European Union, known companies and non-profit companies.

By highest educational level: How much do you trust the following groups of people / institutions to handle your personal data securely?



Concluding remarks

The aim of this report is to inform the public about the motives and views of citizens regarding the handling of their data, especially with regards to digital identities. The results of a representative survey of the German population were presented and briefly discussed. It can be summarized that citizens consider the actual benefits of identity solutions to be most important and, to this end, also provide personal data - for example, to log in securely. It turns out that uncertainty is a major risk factor with regard to the self-assessment of data security on the internet. People see it as a major risk that their data could be used without their consent or without their knowledge. The general perception is that companies as well as governmental institutions and organization are rather not trustworthy in the secure handling of personal data. As already concluded in previous studies, it can be said that a strong confidence in digital offerings is a central acceptance factor in Germany.

This insight serves as an indication that research on secure digital identities, such as in STEREO, is a necessity. Data security and protection is an interdisciplinary topic, which includes social, economic and technical aspects. In the process of developing secure identity and data solutions, it is important to involve citizens in the process in order to meet their needs, which ultimately leads to higher and faster acceptance. In addition to involving citizens, projects should also inform the public and especially citizens about important issues so that they become aware of their potentially unknown problems in dealing with data and identity on the internet.