KIT SCIENTIFIC REPORTS 7753

Attitudes towards big data practices and the institutional framework of privacy and data protection

A population survey

Carsten Orwat und Andrea Schankin

KIT Scientific Publishing

Carsten Orwat and Andrea Schankin

Attitudes towards big data practices and the institutional framework of privacy and data protection

A population survey

Karlsruhe Institute of Technology

KIT SCIENTIFIC REPORTS 7753

Attitudes towards big data practices and the institutional framework of privacy and data protection

A population survey

by

Carsten Orwat

Karlsruhe Institute of Technology, Institute for Technology Assessment and Systems Analysis

Andrea Schankin

Karlsruhe Institute of Technology, Institute of Telematics

KIT Scientific Publishing

Report-Nr. KIT-SR 7753

The survey is part of the project "Assessing Big Data" (ABIDA), which receives funding from the Federal Ministry of Education and Research (BMBF), Germany (grant no. 01IS15016A-F).
http://www.abida.de

abida
ASSESSING BIG DATA

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Impressum

KIT Scientific
Publishing

Karlsruher Institut für Technologie (KIT)
KIT Scientific Publishing
Straße am Forum 2
D-76131 Karlsruhe

KIT Scientific Publishing is a registered trademark
of Karlsruhe Institute of Technology.
Reprint using the book cover is not allowed.

www.ksp.kit.edu

Print on Demand 2018 – Gedruckt auf FSC-zertifiziertem Papier

ISSN 1869-9669
ISBN 978-3-7315-0859-5
DOI 10.5445/KSP/1000086677

Abstract

The aim of this study is to gain insights into the attitudes of the population towards big data practices and the factors influencing them. To this end, a nationwide survey (N = 1,331), representative of the population of Germany, addressed the attitudes about selected big data practices exemplified by four scenarios, which may have a direct impact on the personal lifestyle. The scenarios contained price discrimination in retail, credit scoring, differentiations in health insurance, and differentiations in employment. The attitudes about the scenarios were set into relation to demographic characteristics, personal value orientations, knowledge about computers and the internet, and general attitudes about privacy and data protection. In contrast to the usual context specificity of privacy issues, we observed relatively uniform attitudes across the four scenarios. Some of the features of big data practices, such as the use of data from the internet (e.g., from online social networking sites), automated decision-making by computers in the situations described, and the selling of the data to other companies, were unambiguously rejected irrespective of demographic characteristics, personal values or other investigated factors of the respondents. Furthermore, the anticipated personal advantage of big data-based differentiation and personalisation is minor compared to the suspicion that companies would only try to increase their profits. As one of the consequences, respondents demand easy control options and regulations by the state.

Another focus of the study is on the institutional framework of privacy and data protection, because the realization of benefits or risks of big data practices for the population also depends on the knowledge about the rights the institutional framework provided to the population and the actual use of those rights. As results, several challenges for the framework by big data practices were confirmed, in particular for the elements of informed consent with privacy policies, purpose limitation, and the individuals' rights to request information about the processing of personal data and to have these data corrected or erased. In the light of big data practices perceived, respondents would even change their behaviour when using the internet. This result is contrary to the intentions of the fundamental right of informational self-determination to ensure a free and autonomous development of personality and free speech and opinion in informational contexts.

Keywords: survey, big data, differentiation, personalisation, behavioural adaptations, automated decision-making, informational self-determination, data protection, privacy, notice and consent, purpose limitation, law, institutions, chilling effects

Table of contents

List of tables

List of figures

1 Introduction

The study is aimed at eliciting attitudes of possibly affected individuals towards big data practices, their knowledge about core elements of informational privacy and data protection regulation, and their expectations associated with them. Literature and previous work suggest a sceptical view of the population on big data practices. The study is intended to (1.) analyse the sceptical view and gain insights into factors influencing it. Therefore, the study focuses on big data applications with personal data that have direct consequences for the individuals affected, mainly by differentiation and personalization of offers or rewards. The many definitions, understandings, and general ambiguity of the term 'big data' do not allow for direct work with this term in a survey. Instead, we will use scenario descriptions of big data features that are deemed to most likely have consequences for those who are targeted by the applications of big data techniques and related business practices. (2.) If and how such consequences cause benefits or risks for individuals is dependent upon the institutional and regulatory framework of privacy and data protection and how individuals use it. Within the institutional framework, individuals have legal rights to reach for informational self-determination, but also the task and responsibility to exercise the rights. Thus, in order to gain insights about consequences and potential reactions on big data practices, the study also addresses the knowledge about the rights and the exercising of them, and also if individuals demand improvements of the institutional framework in the light of the depicted big data practices.

The report is organised as follows. Section 2 contains the understandings of 'big data' that are relevant to this study and Section 3 describes big data-based differentiation and personalisation. Section 4 deals with the fundamentals, main principles, and instruments of the European and German institutional and regulatory framework of privacy and data protection that are set into relation with the big data developments and related social concerns. Section 5 provides a brief overview of other relevant empirical research, Section 6 describes the survey approach and methods, while Section 7 delivers the results that are discussed in Section 8. In Section 9, the limitations of the study and suggestions for further research are given.

2 Understandings of big data

Based on the many approaches to explore, define, and delineate the term and concept of 'big data' (Laney 2001; Davenport, Barth and Bean 2012; Chen, Mao and Liu 2014; boyd and Crawford 2012; Zuboff 2015; Constantiou and Kallinikos 2015, p. 49; Kitchin and McArdle 2016; Kitchin 2014; Ekbia et al. 2015; Fosso Wamba et al. 2015), we consider the following features of big data as relevant in this study: (1) the collection, storing, and processing of large volumes of data, here, personal data, (2) the combinatorial and integrating use of such data sets stemming from different social contexts, (3) the automation not only of data collection and processing, but also of analyses, inferencing and, increasingly, decision-making, and (4) the intention to use big data applications in a predictive manner and to differentiate individuals or groups of individuals for differential treatment, among others to influence the behaviour of targeted individuals. This is not a defining and exhaustive list of features of big data, but features that are deemed relevant in terms of (potential) consequences for individuals.

Due to the rapid technological developments, the thresholds to distinguish between 'normal' or small data volumes and those that can be labelled 'big data' are continuously changing (Ekbia et al. 2015). Another trait of big data is the combinatorial use of large-scale sets of often heterogeneous data mostly in different, i.e. structured, semi-structured or unstructured data forms and originating from different informational and social contexts (boyd and Crawford 2012). An example of such 'category-jumping' (Horvitz and Mulligan 2015, p. 254) is the use of data streams from wearables worn in home and leisure contexts for medical purposes. In marketing, business actors intend to gain comprehensive profiles of customers and the so-called '360 degree view' on them by integrating data from different online and offline marketing channels and publicly available data found in the internet or official statistics (Barton and Court 2012; Singer 2012). For such purposes, data brokerage and information reselling are gaining importance concomitantly with developments of big data (FTC 2014; Christl and Spiekermann 2016; Christl 2017).

Of the many potential big data applications, we focus on those in businesses and with processing of personal data, i.e. data that can be related to an identified or identifiable person, who is also called 'data subject' in legislation. In the last decades, the sources of personal data increased significantly through ongoing computer mediation in organisations and inter-organisational relations, in social, economic or financial interactions, and in public and private lives encompassing social communications, houses, vehicles, leisure gadgets, and environments, etc. Together with the use of location data from portable devices, the commercial surveillance of individuals' uses of the internet has become one of the major sources of big data. This includes the massive use of data from social media, search engine queries, web browsing histories and activities, e-commerce, online financial transactions, electronic payment systems (including mobile ones), online comments and reviews, and the use of online services like music or video streaming (Weichert 2013; Constantiou and Kallinikos 2015; Christl 2017; Matz and Netzer 2017; Varian 2010; Eurostat 2016; Röttgen 2018). Often, such data collection is part of the prevalent approach of online marketing based on obtaining 'personal data as counter-performance' for the supply of 'free' online services (e.g., search engine uses) or content products (e.g. newspaper content) (critical on this approach (EDPS 2017)).

The use of mobile communication and smartphones, including the generation of location data, and the use of 'smart' devices of the 'internet of things' with sensors and network connections, such as smart TVs, smart cars, smart houses, smart meters, wearables, activity and health trackers, and other electronic gadgets like e-books, etc. lead to an unprecedented digitisation of individuals' activities and states enabling a shift towards "... datafying and commercializing the everyday" (Kallinikos and Constantiou 2015, p. 71). Such data volumes and data streams are often passively collected, as a more or less transparent element of the product or service, collected within one social context of intimate living conditions, and transferred to central servers or clouds to combine them with data from other contexts.

Not only the sheer quantity of data, especially that of streaming data and continuously or frequently updated data, but also the intention to process data and responses in 'real time' or 'near real time' necessitate more automation in data processing, inferencing, predicting, and decision-making (Kitchin and McArdle 2016; Kallinikos and Constantiou 2015, p. 72f.). Reasons for substituting personal case-by-case judgements and decisions by automatic software-based decision-making, e.g. in scorings and ratings of individuals, are to increase efficiency, to base decisions on a larger set of data, and to prevent human errors and biases in decision-making.

3 Differentiation and personalisation based on big data

Big data applications with personal data are intended to be used among others to differentiate individuals into groups, categories, segments, outliers or single persons, to treat them differentially and, in the end, to influence the individuals' behaviour by economic incentives like price differentiation or by 'nudging', i.e. by providing and delimiting the architectures or scope of choices of the targeted individuals (Yeung 2016; Rouvroy 2016, p. 9ff.). Big data technologies, including artificial intelligence and in particular machine learning, considerably reduced the costs of prediction through the processing of large volumes of learning data in order to extract typical patterns (Agrawal, Gans and Goldfarb 2016). Such patterns can be recognized again in monitored situations or for monitored individuals to predict future states or developments, such as the likelihood of reacting on an advertisement, buying a product or service, repaying a loan, delivering certain work results, or leaving the company. Many of the above-mentioned developments of digital technologies and the internet have also reduced the costs of tracking the behaviour, traits, and states of individuals and of the better verification of their identity (Goldfarb and Tucker 2017). For instance, big data in marketing with data mainly from internet sources is developed to identify and predict the consumers' psychologically stable traits (e.g. personality, IQ or political orientation) and variable states (e.g., moods) in order to target them by personalised advertising or personalised offerings of products or services (Matz and Netzer 2017; Matz et al. 2017).

Overall, differentiation, customisation, and personalisation are possible at lower costs and in finer detail, in constantly experimental ways (Varian 2014), and along new criteria, such as individual characteristics or expected behaviour, with the purpose of generating economic revenues or for economic risk management. Although group- or person-related differentiation of products, services, and prices has a long tradition in market economies, the societal and welfare effects of differentiation with and without big data are ambiguous. On the one hand, groups or individuals can receive more tailored offers of information, products or services, reducing the amount of unused information, such as in advertising, granting lower prices to specific groups or individuals, or leading to higher identification with or demand for products and services. On the other hand, criticism of big data-based differentiations, categorisations and scoring emphasizes the potentials to inappropriately exploit willingness-to-pay and consumer surplus, risks of new forms of 'social sorting' potentially with adverse or illegitimately discriminating outcomes, such as the risks to illegitimately discriminate certain or even protected groups (e.g., Citron and

Pasquale 2014; Rouvroy 2016; The White House 2016; FTC 2016; Barocas and Selbst 2016; Horvitz and Mulligan 2015, p. 254; Carmichael, Stalla-Bourdillon and Staab 2016; Zarsky 2014). Differentiation may also limit available choices and may have implications for the individual autonomy and social justice (Barocas and Nissenbaum 2014, p. 54). Big data-based differentiation could be done along new and non-transparent criteria that challenge or substitute traditional criteria of social differentiation, which are negotiated and widely accepted by society like those of social neediness (Rouvroy and Poullet 2009, p. 16).

Due to their controversial implications of high economic potential as outlined by public, business, and academic discussions, but also their multiple risks and social concerns, the big data practices for differentiations of pricing in retail, credit scoring, tariff differentiation in health insurance, and differentiations in employment are selected as topics of the survey. In particular, discussions relating to differentiations address the potentials and risks of *price discrimination* based on big data, including the use of personal data. Big data practices with personal data can enable first-degree price discrimination in the form of personal pricing that is usually considered a theoretical ideal and is hard to find in practice. Real examples are personalised prices in online shops or offline with personalised discounts or premiums in loyalty programmes or with dedicated smartphone apps. Big data practices also can facilitate third-degree price discrimination with different prices for different groups or types, while the second-degree price discrimination with quantity discounts is deemed less relevant for big data (US CEA 2015; Miller 2014; Ezrachi and Stucke 2016; Steppe 2017; Acquisti, Taylor and Wagman 2016; Zuiderveen Borgesius and Poort 2017; Christl and Spiekermann 2016, p. 41ff.; Schwaiger and Hufnagel 2018; Zander-Hayat, Reisch and Steffen 2016; Tillmann and Vogt 2018).

Another focus of discussions is on *credit scoring* based on big data practices, including the use of social media data, also addressing the limits of the current regulatory framework of data and privacy protection to protect individuals or consumers (Weichert 2014; ULD and GP Forschungsgruppe 2014; Hurley and Adebayo 2016; Ferretti 2017; Wei et al. 2016; Christl 2017; Eschholz 2017). The big data-related debate also comprises *differentiated tariffs for health insurance* based on the monitoring of body data, behaviour or activities through wearables and smartphones so as to enable the person-related provision of incentives for behaviour deemed healthier by adjusting premiums (or sanctioning unhealthier), to sort individuals into certain risk categories, and to select and determine tariffs or premium paybacks individually according to risk estimates predicted. In these debates, also the ethical concerns of such practices, in particular the endangering of solidarity among the insured or redistributional effects, have been addressed (Weichert 2018; Deutscher Ethikrat 2017; ten Have 2013; Christl and Spiekermann 2016, p. 35ff.; Arentz and Rehm 2016; Bitter and Uphues 2017; Swedloff 2014). Furthermore, *big data practices in employment* or human resources (HR) management, also termed 'talent analytics', 'people analytics', 'workplace analytics', or 'HR analytics', including the use of data from (professional) online social networking sites, are subject of intensive debate. Actual and intended usages of big data practices range from investigating job candidates to investigating the compliance of employees, selecting applicants, incentivise employee performance, or promoting or binding employees (Rosenblat, Kneese and boyd 2014; Burdon and Harpur 2014; Marler and Boudreau 2017;

Chamorro-Premuzic et al. 2016; Chamorro-Premuzic et al. 2017; Dzida 2017; Weichert 2018, pp. 59-61; Angrave et al. 2016). Examples of big data applications in talent analytics include machine learning algorithms that process and evaluate 'digital footprints' especially from social media data as well as the use of digital interviews, i.e. interviews recorded and analysed with technologies of 'social sensing' (Chamorro-Premuzic et al. 2017).

4 Institutional framework of data protection and social concerns

4.1 The fundamental right of informational self-determination

In Europe and Germany, a comprehensive and detailed institutional framework for data and privacy protection regulates the collection, processing, and transfer of personal data, including big data practices. In Germany, the constitutional right to informational self-determination, serving the protection of human dignity and based on the general rights of personality derived from Article 2, par. 1 in connection with Article 1, par. 1 of the Basic Law for the Federal Republic of Germany, establishes the objectives and principles underlying the legal provisions of privacy and data protection.

The *right to informational self-determination* ensures the authority of the individual to principally determine for herself or himself the disclosure and use of her or his personal data (see decision by Federal Constitutional Court, BVerfG 1983, p. 43). The goals of the right are to establish an institutional environment of trust necessary for the self-development and unfolding of the individual and to secure all other freedoms, in particular the right to freedom of opinion and speech (Rouvroy and Poullet 2009; Roßnagel and Richter 2016). Conceptually, the goals are to ensure the free development of one's personality in informational contexts and the commitment and free forming of a political will in a democratic society. The free development of personality requires a relative stability of expectations and orientations with regard to social contexts. It includes the possibility to establish and have trust that the limitations of visibility in specific contexts and roles are ensured, defective data sets or distorted representation of the individual not being sustained, and an outdated past representation not haunting a person without a chance of forgetting. Without a social context that ensures trust in such integrity, a general uncertainty can lead to inhibiting oneself in dealings with others or potentially leading to behavioural self-constraining or behavioural conformity based on expectations about negative consequences. That could result at a level that is incompatible with the free development of one's personality protected by fundamental law (Albers (2017, p. 28) with reference to Nissenbaum (2004, 2010)).

Encroachments on the right to informational self-determination are only allowed when other public interests are deemed to be of higher priority, such as in the case of national security. However, even then encroachments are bound to several principles and provisions, especially the principles of necessity and proportionality, which have to be proven for the encroachment. In general, the state has the fundamental responsibility for ensuring the right to informational self-determination. The right is also relevant for relations of private actors like companies with affected individuals. On the European level, Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (Charter of Rights 2012) and Article 16 of the Treaty on the Functioning of the European Union (TFEU 2012) establish the fundamental right to privacy and data protection.

4.2 Main principles and instruments and questions about their adequacy

On the national level, the fundamental right to informational self-determination is specified by the main principles and instruments of the German data protection regulation, especially the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), revised in 2017 (BDSG 2017), (Simitis 2014; Weichert 2013; Roßnagel and Richter 2016). On the European level, the European General Data Protection Regulation (GDPR) (GDPR 2016) from the year 2018 on and also (later) by the (renewed) e-Privacy Regulation particularly dedicated to electronic communication are the main laws of privacy and data protection. Despite some differences in the conceptual approaches, details in legislations, and in their assumed efficacy, the main principles and instruments of privacy and data protection, which are relevant to this study, are similar in BDSG, GDPR, and the e-Privacy Regulation.

In general, any processing of personal data is prohibited, unless individuals who are affected by the data processing give their unambiguous and voluntary consent to it or a law or legal provision regulates and allows it. In order to give consent, the law requires that the affected individual or data subject is adequately informed in advance so that the individual is able to know what she or he agrees to. According to this so-called *'informed consent'*, 'notice and consent' or 'notice and choice' approach, any processing of personal data requires notice of the affected person so that the person can assess the data processing to be permitted and the consequences of it (Article 4 No. 11, Article 6 par. 1 GDPR; see also the duties to inform in Article 12 to 14 GDPR).

The principle of *'purpose limitation'* or 'purpose binding' prohibits the use of the data for purposes other than stated, including the combined use of data taken from other purpose contexts. Data processing is permitted only for a specific purpose specified either by law or the purpose for which consent is given. A change of the purpose by the data controller requires a separate consent or permit by law. The purpose limitation is the necessary basis for the affected person to control which data are processed. This principle is fundamental, since an individual can only give consent to a purpose that is clear-cut, understandable, and limited. Furthermore, the *principle of 'necessity'*, i.e. of data processing being allowed only with those data, with such forms of data processing, and in such time periods, which are necessary for the legitimate purpose stated, refers to data avoidance and reduction and data minimisation (Article 5 par. 1 lit. b, c GDPR). These principles are further underpinned by the newly introduced concepts of privacy-by-design and privacy-by-default (Article 25 GDPR).

The GDPR (and the revised BDSG) grant individuals several rights when they are affected by a processing of personal data in order to ensure control of the use of data about them. In the following, only those rights directly relevant for the study are described. The data controller also has the duty to provide the necessary information so that the affected person is able to exercise these rights (Article 12 to 14 GDPR). The *right to access* requires that information about the personal data on data subjects stored by the responsible data processing entity, i.e. the data controller, should be made available on request of the data subject (Article 15 GDPR). Further rights enable affected persons to request the *correction* of false data (Article 16 GDPR), the *blocking* of controversial data (Article 18 GDPR), or the *deletion* of inadmissibly processed data. The right to *erasure* of certain data is often called the 'right to be forgotten' (Article 17 GDPR) and also includes the erasure of personal data made public or transferred to other data controllers. Data subjects also have the right to withdraw the given consent at any time (Article 7 para. 3 GDPR). Furthermore, there is also, in principle, a right not to be subject of a decision based solely on the automatic processing of data, including profiling (Article 22 GDPR, see below).

Developments of big data techniques and practices raise several societal concerns and question the adequacy of the existing institutional framework of data protection and privacy regulations and the fundamental goal that individuals can control who knows what about them (Rubinstein 2013; Barocas and Nissenbaum 2014; Horvitz and Mulligan 2015; Roßnagel and Nebel 2015; Weichert 2013; Raabe and Wagner 2016b; Roßnagel et al. 2016; Roßnagel and Richter 2016; Gonçalves 2017). Risks for the principles of *purpose limitation* result from the mostly purpose-less and arbitrary data collection in big data practices as well as from the 'context-jumping' and combinatorial usages of data. In particular, the combinatorial use of different data sets and the application of machine learning enable detailed conclusions with respect to sensitive attributes, states or situations of individuals (e.g. health status or those prone to discrimination) from data previously deemed harmless or publicly available, such as queries on search engines or communication in online social networks (Solove 2013; Horvitz and Mulligan 2015, p. 253f.). This is aggravated by many options of de-anonymisation and re-identification of individuals from non-personal or anonymised data (Ohm 2010; de Montjoye et al. 2015; Barocas and Nissenbaum 2014). In this respect, the protection level of the GDPR is unclear, because in comparison to the BDSG it leaves more room for data controllers to adopt a wide interpretation of what a 'similar purpose' is, for which the use of data would be legal (Raabe and Wagner 2016a, p. 20ff.).

Within the relationship between data controllers and data subjects, multiple *information asymmetries* and differences in cognitive capabilities exist with regard to the technologies of data collection and processing and their actual applications, the volume, type, and quality of the data, the purposes of data processing, the decisions that are based on such data processing, and, thus, the benefits and risks for the data subject as well as the technical and organisational options for enhancement (e.g., Baruh 2007; Acquisti, Taylor and Wagman 2016). The original intention of the *'informed consent'* approach with requirements to provide privacy notices, privacy statements, or privacy policies is to reduce such information asymmetries between individuals and data controllers as well as the resulting differences in knowledge and power and to provide means of 'levelling the playing field'. Additionally, this instrument should be the informational base for enabling data subjects to give an adequately knowledgeable consent, to recognize when their individual rights are affected or infringed, and to enforce them (Rouvroy and Poullet 2009;

Van Alsenoy, Kosta and Dumortier 2014). However, many authors have pointed out *weaknesses of the informed consent* approach, revealing the ambiguity and vagueness of terms used in privacy policies, the formulation mostly in 'legalese' from lawyers to lawyers, the inadequacy of information provided, cognitive hurdles to understand the information, efforts and time constraints to read privacy statements, and that most people just do not read them (Milne and Culnan 2004; Solove 2013; Cate and Mayer-Schönberger 2013; Reidenberg et al. 2015; Reidenberg et al. 2016; McDonald and Cranor 2008b; Van Alsenoy, Kosta and Dumortier 2014; Martin 2013; Moll et al. 2018). Solove (2013) identifies and also demonstrates structural problems, i.e. there are simply too many companies or other entities providing privacy notices, for which giving meaningful consent would be required. More importantly, most privacy harms result from the aggregated and combinatorial use of personal data collected over time and from different sources, which is typically the case with big data practices. This, however, makes meaningful mental cost-benefit analyses in the sense of a necessary balancing of the benefits of disclosing personal information against any future negative consequence, virtually impossible for the affected individual when she or he is required to give consent. Additionally, some societal consequences of using and misusing personal data, such as adverse effects on the freedom of opinion or negative externalities of data disclosures about social relationships on other individuals (typically on online social networking sites), may not be considered in such decisions by individuals. Solove concludes that in particular the inadequacy of the instrument of privacy notices and consent is a main argument for the inadequacy of the current 'privacy self-management' approach in privacy regulation (Solove 2013). Despite the many criticisms, however, current privacy and data protection regulations is still be based on the informed consent approach (e.g., Martin 2016).

The automated execution of decision rules, or *automated decision-making* for short, is seen as one of the traits of big data practices, in particular with profiling or scoring, and has raised social concerns. They range from discrimination by inadequate differentiation, diminishing chances to contest such decisions and for fair trials or due processes in judicial disputes, blurring or covering of responsibilities and liability, prejudices and bias in processing algorithms and data sets, to ambiguous efficiency gains, errors, issues of unfairness and opacity (Article 29 DPWP 2018; Deutscher Ethikrat 2017; Martini 2017; Schneider and Ulbricht 2018; Citron 2008; Citron and Pasquale 2014; Hildebrandt and Koops 2010; Barocas and Nissenbaum 2014; The White House 2014; Barocas and Selbst 2016; Zarsky 2016; Lepri et al. 2017; Mittelstadt et al. 2016).

In principle, the legal right not to be subject of a decision based solely on the automatic processing of data, including profiling, as granted by Article 22 GDPR, addresses such concerns with the prohibition of certain kinds of automated decision-making. Automated decision-making is allowed when it is necessary for entering or executing a contract, when it is authorised by law, or when the data subject gave explicit consent to it (Art. 22 par. 2 GDPR). According to Weichert (2018), the provisions of Art. 22 are relevant, if the automated decision-making process is not based on a pre-defined comprehensible 'if-then' decision, and if this type of decision-making is complex, not transparent, and not controllable, and a revision cannot be made by the affected individuals. This is in particular the case, if the algorithms are not fully documented and, thus, not comprehensible or if the decision-making process is based on artificial intelligence, such as self-learning systems (Weichert 2018, p. 130f.). To be relevant for the prohibition, it is also required that the automated decision-making has legal effects or similar significant effects on the data subject. This might be the case for the big data practices considered in this study, i.e. big data-based price differentiation, credit scoring, and determination of insurance tariffs or premiums or of wages or employment conditions. Together with Article 22 GDPR, the Article 13 par. 2 lit. f, Article 14 par. 2 lit. g, and Article 15 par. 1 lit. h GDPR establish an obligation of the data controller to inform about the involved logic, the significance and the envisaged consequences of the automated decision-making (Weichert 2018, pp. 134, 149f.) (critical on a right to explanation (Wachter, Mittelstadt and Floridi 2017)).

5 Related empirical research

Numerous empirical studies focus on attitudes and concerns about privacy and data protection, of which only a few overviews (Smith, Dinev and Xu 2011; Bélanger and Crossler 2011; Hallinan, Friedewald and McCarthy 2012; Wright et al. 2013; Acquisti, Taylor and Wagman 2016; Baruh and Popescu 2015; Kokolakis 2017) and selected studies can be mentioned here.

Regarding the *general importance of privacy*, European citizens usually considered the privacy of their personal information to be of high importance (European Commission 2016, pp. 29-35). In comparison to other citizens of the European Union, German citizens in particular felt to have lost control of the information they provide online (European Commission 2015). With regard to attitudes and expectations on purpose limitation, primary and secondary uses of personal data, the majority of the European respondents, with 67 percent of respondents from Germany, thought that the collection of their data would require their explicit approval and that their information is used for a purpose other than that it was collected for (European Commission 2015, pp. 58-71). Similar results were obtained for the USA, pointing to people's negative suspicion when data are collected for one purpose, but are used for other, more invasive purposes (Rainie and Duggan 2016).

Another research branch relevant to the study at hand is the research into *reactions or adaptive behaviour* to perceived threats to the individual's privacy, autonomy, and personal freedom, an issue that is also discussed under the term *'chilling effects'*. The research considers the implications of extensive surveillance for negatively affecting the individuals' ability to exercise their liberties to speak, associate, or inquire information (e.g., Baruh 2007; Schwartz 1999). Empirical studies found chilling effects, self-censorship, or negatively directed impression management on social networking sites through surveillance by their audience like family members and friends (Das and Kramer 2013; Lang and Barton 2015) and extensions of the chilling effect to offline environments (Marder et al. 2016). Marthews and Tucker (2017) conducted an empirical study about changes in keywords used in search engines resulting from the revelations by Edward Snowden in 2013 on governmental mass electronic surveillance in partnership with private companies, such as Google, Yahoo, Microsoft, AOL, Skype, and others. They demonstrated the existence of a chilling effect related to surveillance, mostly in terms of a decline in search terms that are deemed personally sensitive (in particular health-related terms) and government-sensitive. Similar studies revealed regulatory 'chilling' effects stifling the freedom of expression and freedom on exchange based on observed changes in the use of Wikipedia articles about privacy issues after the publicity of the NSA surveillance, which were not only of immediate, but also of long-term character (Penney 2016, 2017). Related research considered the tendencies of users to manipulate entries in online social networking sites to produce a better self-presentation on job markets (Schroeder and Cavanaugh 2018).

As regards *attitudes towards and knowledge about responsibilities and legal instruments* of privacy and data protection, surveys show that the population has some, but incomplete knowledge about the legal situation of data protection. 44 percent of respondents from Germany had heard of a public authority responsible for protecting their rights regarding their personal data (compared to 37 percent for the EU28 average) (European Commission 2015, pp. 51-53). A majority of respondents from Germany, who provide information online, thought that online companies are responsible for protecting their personal information, but also individuals themselves and public authorities (European Commission 2015, p. 104ff.). National statistics shows that only 3 percent of German internet users had applied for access to personal information stored on websites of search engines (Statistisches Bundesamt 2016, p. 43). A consumer survey on the right to access to credit scoring data reveals that 43.3 percent were aware of the existence of this right and 84.3 percent were in favour of an active information by the scoring company (ULD and GP Forschungsgruppe 2014, pp. 95, 112).

Empirical studies also investigated the *informed consent approach* and the central role of privacy policies, privacy statements or privacy notices. The majority of respondents to a European survey about online activities knew that personal information (e.g. photos, calendars, or history of queries) on computers, smartphones or tablets can only be accessed, if users give their permission, or similar, that information (e.g. cookies) can only be stored on such devices, if permission is given. However, the majority did not know that the communication in messaging and online voice conversation is not confidential and not protected by law (European Commission 2016, pp. 22-29). According to another study, 17 percent of the respondents from Germany (who use the internet) had fully read privacy statements, 55 percent partly, and 26 percent had not read them at all. Respondents, who said they had read privacy statements only partly, gave reasons for this. In their opinion, these statements are too long as well as unclear and difficult to understand (European Commission 2015, pp. 84-90). National statistics reveals for German internet users that 43 percent of them read privacy statements before transmitting personal information in order to control access to that information on the internet (Statistisches Bundesamt 2016, p. 42).

Further empirical studies reveal, for instance, that reading privacy policies is related to concerns for privacy, positive perception of notice comprehension, and higher levels of trust in the notices, and that it is only one element of consumers' strategy of risk management (Milne and Culnan 2004). Another study found that users agree to privacy notices and terms of services even when joining a fictitious online social networking site was associated with sharing personal data with surveillance agencies and offering their first-born child (Obar and Oeldorf-Hirsch 2016).

Further research concluded that respondents deemed the privacy notice a greater protection than it actually was (Martin 2015), and that the mere introduction of formal contracts with privacy notices decreased trust and caused respondents to suspect websites of violating informal privacy norms (Martin 2016). Considering the practices of using privacy policies, a study covered the relatively high efforts for individuals to read privacy policies (McDonald and Cranor 2008a). Another study analysed the privacy notices of 75 online tracking companies as to whether they provided information relevant to users for making privacy decisions and found that many did not contain information about important consumer-relevant practices (Cranor et al. 2014). However, an online experiment and field study with additional short privacy statements, so called 'one-pager', showed, among other things, that the state of being informed does not increase significantly with the use of additional one-pagers (Kettner, Thorun and Vetter 2018) .

Several studies cover the *attitudes, acceptance, concerns or expectations of business practices* that affect the privacy of individuals or parties. A survey shows that the willingness to engage in online transactions of e-commerce is influenced by the individuals' information on privacy concerns, but is also determined by risk perception and trust, with the latter being based on the familiarity with the online merchant (Van Slyke et al. 2006). Niemann and Schwaiger (2016) explored the factors that influence consumers' expectations about a fair data collection and usage by in-depth interviews of customers and experts as well as an online survey among German consumers. The results reflect the customers' expectations to get simplified privacy statements and easier control options. The study also reveals that customers' expectations were underfulfilled and that consumers were willing to switch to competitors that better fulfil their expectations.

Surveys on the attitudes towards differentiation, personalisation, and business practices with providing personal data as 'counter-performance' reveal that people feel uncomfortable with tailored advertising based on the collection and processing of personal data in return for free online services (European Commission 2015, pp. 39-41; Statistisches Bundesamt 2016, p. 44; Turow et al. 2009) and that they tend to reject price discrimination based on processing of data gathered from online activities (Turow, Feldman and Meltzer 2005). The majority of respondents of the 'e-Privacy' survey said that they would accept neither having their online activities monitored in return for unrestricted access to a certain website, nor the sharing of personal information without permission in return for new service offerings, nor the paying for not being monitored when using a website (European Commission 2016, pp. 55-60). Rainie and Duggan (2016) present findings from a survey of American adults that suggest that such trade-offs in business contexts about the willing to disclose and share personal information in return to received benefits is contingent and context-dependent.

With regard to privacy issues on job markets and in employment relations, empirical studies considered, for example, the students' awareness of and expectations associated with the use of social media data by prospective employees (Root and McKay 2014), ethical decisions and reactions by job applicants to such practices (Drake et al. 2016), attitudes towards the use of online social networking sites in recruiting (Vicknair et al. 2010), or the employees' privacy concerns about or respondents' sensitivity to different types of information typically stored in computer-based human resources information systems (Taylor and Davis 1989; Lukaszewski, Stone and Johnson 2016).

Empirical studies have also started to *explicitly focus on big data*. An online survey (N = 202) in 2014 reveals, among other things, the ambiguous attitudes about big data in terms of advantages and disadvantages, a lack of trust in big data-relevant industries, the insufficient implementation of data protection regulations, and demands for modernised and additional regulations (Steinebach et al. 2015). A population survey of European citizens, including German citizens (N = 1,216), conducted in 2015 covered four scenarios of (1) connected cars and the different uses of car data, (2) different uses of data from loyalty cards in retail, (3) uses of patient data in health care and health insurance, and (4) uses of data about energy consumption from smart meters. As a generalised result, the survey shows a sceptical view of citizens regarding the described big data practices and, in particular, a strong disapproval of the transfer to and secondary use of data by third parties, even in anonymised form (Vodafone Institut 2016). Another survey on big data practices considered the extent of such practices, the loss of trust, and the 'misuses' of data and pointed out that consumers are unpleasantly surprised when they recognize that personal data are collected and used for a purpose other than the original one (Umhoefer et al. 2015). A survey with the explicit focus on big data explored the opinions and expectations of experts and stakeholders, including promising applications and implications for governance (Jarchow and Estermann 2015). An online survey covering the attitudes about automated decision-making shows that the majority of the population (weighted, N = 5,040) agreed to the statement that automated decision-making by algorithms are a danger, to the necessity of disclosing data and criteria of such decision-making, and to the need for political intervention and regulation and for the state to investigate compliance with the law (Braun 2017). Focusing on algorithms employed in a wide range of applications from automated spellchecking to automated judgements on risks of recidivism of offenders, a survey by Fischer and Petersen (2018) revealed, among other things, that respondents mainly reject completely automated decision-making for the majority of applications and that the respondents agree to a range of governance measures including a right to demand information, a duty to label algorithmic decision-making, or a prohibition of completely automated decision-making by computers.

6 Survey

6.1 Context

The survey was part of the government-funded research project 'ABIDA – Assessing Big Data', which has the aim to identify and assess impacts of big data developments on society. The project relies on the problem-oriented approach of technology assessment by analysing the changes in societal structures caused by technological developments and their intended and unintended consequences (e.g., Grunwald 2009). Analyses also include the exploration of necessities and options to react to possible innovation hurdles and possibly identified risks for society, governance options or necessary adaptations of the legal framework.

The survey was embedded in a mixed-method approach of the entire project and was based on several other work packages, in particular on results of three citizens' conferences conducted in the year 2016 to elicit citizens' views, concerns, and hopes relating to big data. At all three citizens' conferences, the participating citizens expressed more concerns than hopes about big data. They primarily demanded more information and educational measures in the sense of training competences to cope with the opportunities and risks of digital media, including big data, and their management of personal data. In the opinion of the citizens, education should start in elementary school and extend to adult education. Furthermore, participants requested more governmental regulation and saw the government to have a central responsibility for an effective regulation of big data applications, to avert dangers by heteronomy and ensure civil rights and liberties, and to impose strict sanctions in cases of legal infringements. Requested governmental tasks also included the provision of a legal framework, in which individuals can better assume their self-responsibility for data protection especially with the help of rights to information or transparency about data streams, support of the development of alternatives and options of choice if market outcomes are deemed insufficient, as well as the enabling of differentiated forms of consent to the use and transfer of personal data, in particular medical data. Many participants did not have concrete understandings of the term 'big data' and rarely related the term to actual examples or issues of big data practices (Hügle 2017).

Further previous work on the basis of which the survey was developed included an extensive literature review, scientific reviews of big data topics in disciplines of social sciences, namely ethics, law, economics, sociology, and political science (Kolany-Raiser et al. 2018), as well as a Delphi workshop with experts in the areas of privacy and data protection, politics, business, and science (König 2016).

6.2 Focus and research questions

The focus of the survey was on big data practices that might generate *direct consequences* for individuals in their roles as consumers, employees, insured, or citizens. Other big data applications, such as in production, logistics, law enforcement, or national security, were not considered. Due to the high economic potentials, but also their considerable risks, the focus was on big data practices in business with gathering, appropriation, processing, and commercialisation of *personal data* and with possible consequences of big data practices on individuals. Since such practices are considered to pose risks for fundamental values and rights and, thus, are usually addressed by the institutional framework of legal protection rights and duties, this framework was also investigated with respect to big data practices.

Against the backdrop of previous research on the aforementioned big data practices, societal concerns, and questions about the adequacy of the existing legal framework of data protection, the following *research questions* (RQ) were formulated:

RQ1: Can some features of big data practices be identified, which contribute in particular to the sceptical attitude?

RQ2: Can individuals be differentiated with respect to their sceptical attitude on big data practices?

RQ3: In view of the exemplified big data practices, what are the opinions of the population with regard to the institutional framework of privacy and data protection or other measures required?

RQ4: Can individuals be differentiated with respect to their opinions on the institutional framework?

6.3 Methods

6.3.1 Survey design

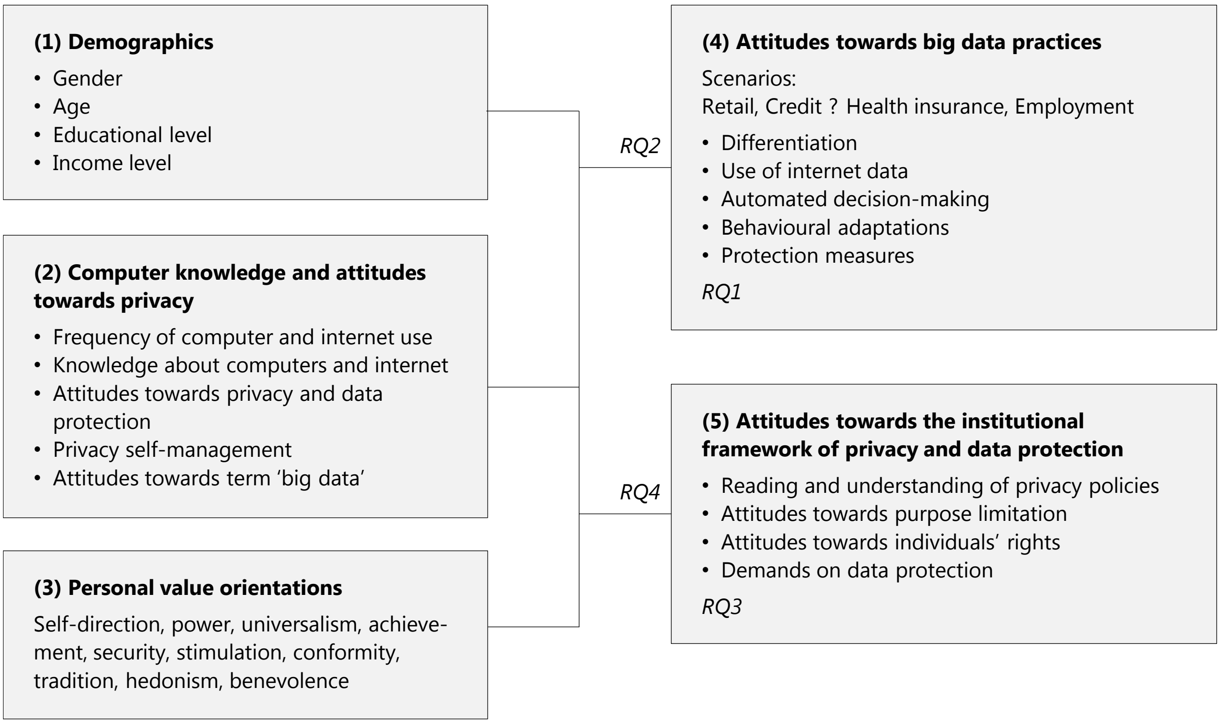
The study used an *explorative research approach* for attitudes towards big data practices that were not well observed, understood, or theoretically backed. Therefore, the public opinion survey did not only use traditional survey questions, but also four scenarios, i.e. descriptions of situations in which big data practices are applied.

To answer the research questions, the survey was designed to consist of five main parts (overview in Figure 6.1): (1) demographics, (2) computer knowledge and attitudes towards privacy, (3) personal value orientations, (4) attitudes towards 'big data' practices described in the form of four scenarios, and (5) attitudes towards the institutional framework of privacy and data protection. The variables of demographics (1), computer knowledge and attitudes towards privacy (2), and personal value orientations (3) will hereinafter be considered as moderators for the attitudes towards big data practices and towards the institutional framework of privacy and data protection.

(1) *Demographics (potential moderators: RQ 2 and RQ 4):* To describe the sample, we gathered data about demographic variables, i.e. gender, age, educational level, and income level.

(2) *Computer knowledge and attitudes towards privacy (potential moderators: RQ 2 and RQ 4)*: Our study also included the frequency of computer and internet usage, general attitudes about data protection and measures taken for self-management in data protection, as well as knowledge about the term 'big data' and expectations associated with it as potential moderators.

(3) *Personal value orientations (potential moderators: RQ 2 and RQ 4):* Personal value orientations of interviewees were measured with the standardised Human Values Scale developed by Shalom Schwartz. We used the standardised 21-items measure of the Portraits Value Questionnaire (PVQ) for ten values (see Table 7.3, page 22) (Schwartz 2003b, 2003a; Schwartz, Breyer and Danner 2015). In this questionnaire, respondents indicate how similar they see themselves to described portraits representing certain personal values. The value orientations of the respondents are indirectly inferred from their statements about the similarity (Schwartz, Breyer and Danner 2015).



(1) Demographics

- Gender
- Age
- Educational level
- Income level

(2) Computer knowledge and attitudes towards privacy

- Frequency of computer and internet use
- Knowledge about computers and internet
- Attitudes towards privacy and data protection
- Privacy self-management
- Attitudes towards term 'big data'

(3) Personal value orientations

Self-direction, power, universalism, achievement, security, stimulation, conformity, tradition, hedonism, benevolence

RQ2

RQ4

(4) Attitudes towards big data practices

Scenarios:
Retail, Credit ? Health insurance, Employment

- Differentiation
- Use of internet data
- Automated decision-making
- Behavioural adaptations
- Protection measures

RQ1

(5) Attitudes towards the institutional framework of privacy and data protection

- Reading and understanding of privacy policies
- Attitudes towards purpose limitation
- Attitudes towards individuals' rights
- Demands on data protection

RQ3

Figure 6.1: Overview of the survey design

(4) *Attitudes towards big data practices (scenarios; RQ1 and RQ2):* The core of the survey were questions on attitudes towards some features of big data practices, namely, targeted differentiation, combinatorial use of personal data from different sources, including the internet, automated decision-making, and possible reactions to and expectations on such practices.

Preceding empirical studies revealed that attitudes towards privacy and data protection are often expressed generically on an abstract level, while the actual behaviour and behavioural intentions are more dependent on and modulated to specific contexts or situations (Nissenbaum 2011; Acquisti, Brandimarte and Loewenstein 2015; Acquisti, Taylor and Wagman 2016; Martin and Nissenbaum 2016; Kokolakis 2017). Therefore, the scenarios depicted different situations of big data practices in specific contexts, for which interviewees had to make mental trade-offs between potential benefits and risks by their involvement in these described practices. The selection of the scenarios was by no means exhaustive of all types of big data applications in business, but was to represent situations with direct impacts on individuals, in particular on presumed options of their personal self-development.

Although the scenarios were developed in view of actual cases and examples of big data practices, we assumed that they can be considered hypothetical situations for the majority of respondents, especially because of the assumed lack of individuals' knowledge about current data processing practices. Furthermore, the specific institutional and legal conditions of countries had to be considered to estimate the realisation of the scenarios. Although the German legal framework of data protection was deemed to be relatively detailed and enforced, the big data practices portrayed may also become relevant to the population of the survey, at least, as possible applications with potential benefits or risks. For instance, the decision by the Federal Labour Court (Bundesarbeitsgericht, judgement of 27th July 2017, 2 AZR 684/16), which prohibits the exhaustive and continuous surveillance of employees with the help of surveillance software ('keylogger') or the legal requirement to have data protection officers at the worksite (beyond certain criteria met by companies) (Article 37 GDPR) limited the immediate realisation of the employment scenario, but was discussed as a potential big data application in the public debate.

The scenarios portrayed situations with the above-mentioned relevant features of big data practices. Data collection led to a constant stream of data for profiling used to differentiate outcomes for individuals and for automated decision-making. Data sets for the combinatorial uses included personal data relevant to personal self-development, which resulted from monitoring online activities, such as communication in online social networks. The scenarios also included data usually considered sensitive, i.e. vital data in the 'health insurance' scenario, financial data in the 'credit scoring' scenario, and employment information in the 'employment' scenario.

(5) *Attitudes towards the institutional framework of privacy and data protection (RQ3 and RQ4):* Literature on social concerns and legal treatment of big data practices points to their risks for fundamental values and rights and highlights challenges for the existent institutional framework of data and privacy protection regulations, as summarised above. Therefore, the study covered the population's knowledge about the institutional framework, its principles, instruments, and rights, their use by the population, and demands for improvements. The focus was directed towards the principles and instruments considered to be most relevant from the perspective of individuals (potentially) affected by big data practices, i.e. the 'notice and consent' approach with the instrument of privacy policies, the principle of 'purpose limitation', issues of trust in the companies obeying to them, and the individuals' rights to request access to or information about data processing when affected by it as well as correction or erasure. Here, the study also contained considerations of possible influences of the moderators on differences in awareness, knowledge, and use of the institutional framework as well as expectations associated with it.

6.3.2 Procedure

The survey was conducted by professionally trained interviewers of a social and market research company in the form of computer-aided telephone interviews (CATI) from February 2017 to April 2017. The target population was inhabitants of Germany aged 18 years and more, who were randomly selected by using the sampling approaches ADM eASYSAMPLe (based on the Gabler-Häder method) for landline connections and eASYMOBILe for mobile connections.

The survey follows the guidelines of the Arbeitsgemeinschaft Deutscher Markt- und Sozialforschungsinstitute e.V. on conducting telephone surveys. At the beginning of the telephone call, interviewees were informed about the scientific purpose of the interview, the identity of the survey organization, the type of content of the questions, and the voluntary nature of participation. The interviews contained a consent question that needed to be answered before participants could begin the survey. All interviewees participated voluntarily and had in anytime the option to end the telephone interview. They did not receive any payment or other remuneration. The survey data were gathered and processed in anonymized form.

The 1,331 completed questionnaires comprise 44.2 percent mobile and 55.8 percent landline phone respondents. Most questions had options to answer with a 5-point rating scale (Likert-like) anchored with 'Fully agree' to 'Do not agree at all', or 'Very uncomfortable' to 'Very comfortable', for instance (see Appendix B: Questionnaire). The average length of an interview was 34.7 minutes (median = 34 minutes). Responses by the interviewees were weighted to obtain a representation of the entire German population. To this end, standard weighting procedures were applied to reduce differences between the sample and the entire population with regard to known rates of response and non-response depending on household size, age, gender, educational level, and place of residence.

Questions about attitudes towards data protection in general were asked before the big data scenarios in order to avoid distortion through the scenarios. Further questions about the institutional data protection framework were deliberately placed behind the big data scenarios to elicit the opinions about its adequacy in the light of the big data practices described. Knowledge of and expectations associated with the term 'big data' were asked for after the scenarios in order not to influence the answers relating to the scenarios.

The scenarios were presented to the interviewees in brief explanations (see Appendix B: Questionnaire). At this position of the questionnaire, the total set of respondents (N = 1,331) was split into two randomly sorted groups. To each subset two scenarios were presented, i.e. 'retail' and 'credit' to one subset (N = 662) and 'health insurance' and 'employment' to the other subset (N = 669). Every scenario had similar types of questions to elicit and compare the opinions about (1) differentiation and personalisation in general, (2) big data-based differentiation with the use of data from the internet, (3) automated decision-making in the situation described, (4) possible adaptations of behaviour in response to the use of data from the internet, and (5) possible measures demanded and expected by the affected individual in view of such practices. A second split of interviewees was for the exploration of personal value orientations in female and male interviewees to be asked with a dedicated questionnaire.

6.4 Demographics

Table 6.1 shows the demographics of the survey sample. Regarding the education level, the survey asked for the highest educational qualification, which is usually differentiated in general education and vocational education. The responses were regrouped according to the International Standard Classification of Education (ISCED 2011) into 'low', 'medium', and 'high' education levels (OECD 2015; Statistisches Bundesamt 2016).

Table 6.1: Demographics

Category		Frequency	Percent (%) of population
Gender	Male	650	48.9
	Female	681	51.1
Age[a]	18-19	41	3.1
	20-29	188	14.1
	30-39	184	13.8
	40-49	211	15.9
	50-59	256	19.2
	60-69	231	17.4
	70-79	153	11.5
	above 80	67	5.0
Income[b]	Below 1,000 Euros	183	13.7
	1,000 to 2,000 Euros	350	26.3
	2,000 to 3,000 Euros	303	22.7
	3,000 to 4,000 Euros	130	9.8
	4,000 Euros and more	147	11.1
	Not stated	218	16.4
Education	Ongoing education	77	5.8
	Low	91	6.8
	Medium	681	51.2
	High	476	35.8
	Not specified	6	0.4

Notes: N = 1,331. Values are weighted to represent the entire German population.
[a] Values for age were regrouped into the cohorts shown.
[b] Monthly net household income.

7 Results

7.1 Potential moderators

7.1.1 Frequency of computer and internet use

Table 7.1 depicts the frequency of computer and internet usage by the German population. The observations were similar to those of official population surveys on the European (European Commission 2016) and national level (Statistisches Bundesamt 2016), indicating a high usage in terms of usage time and total population.

Table 7.1: Frequency of computer and internet use

Frequency of use	Frequency	Percent (%)
Practically the whole day	234	17.6
Several times during the day	708	53.2
Several times during a week	133	10.0
Once per week	37	2.8
Less frequent	49	3.6
Never	166	12.5
Not stated	5	0.3

Note: N = 1,331 (weighted).

7.1.2 Self-assessment of knowledge about computers and internet use

Figure 7.1 presents the computer and internet literacy of the population as self-assessed by the respondents for the question "How would you assess your knowledge of computers and the internet?" regarding different usage types and devices. Although usage of smartphones and tablets in the population generally is relatively high, the survey revealed that respondents self-assessed their knowledge of using the internet with PCs or PCs in general was highest (numerical values in Table A.1 in Appendix A).

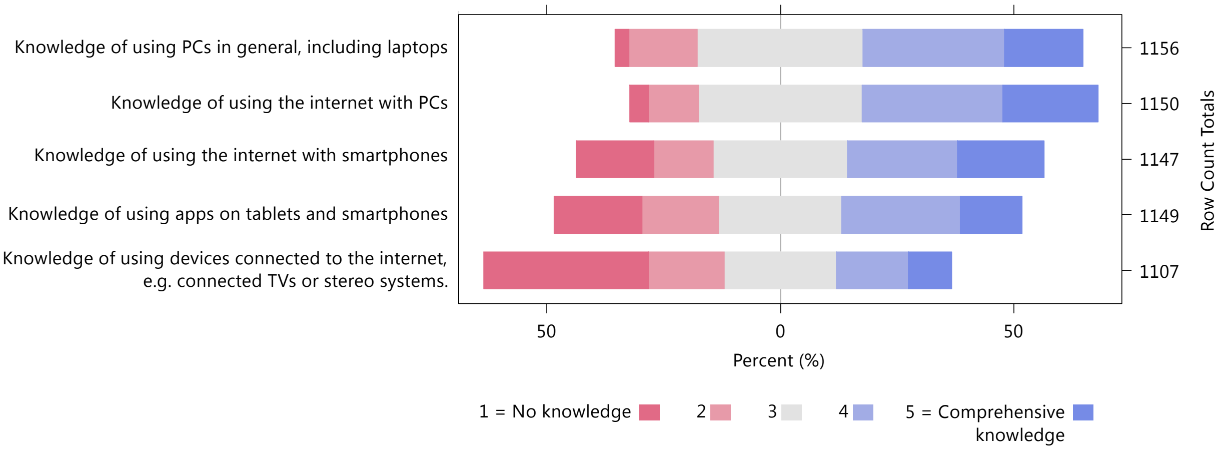


Figure 7.1: Self-assessment of knowledge about computers and internet use

Notes: N = 1,331. 170 respondents with no computer and internet use or with no answers not shown here. Items were read in random order to respondents.

7.1.3 Attitudes towards privacy and data protection

The questionnaire asked for the attitudes towards privacy and data protection with several detailed abstract statements, to which respondents indicated their level of agreement or disagreement (see Questionnaire in Appendix B). The observations, shown in Figure 7.2 as percent of the population, indicated that a majority was concerned about data and privacy protection in general and about what happens to their personal data in particular. This is indicated not only by a large portion of agreement with statements expressing concerns, but it is also confirmed by a high percentage of disagreement with statements for resignation and ignorance about data protection. Furthermore, a portion of 48.1 percent disagreed with the 'personal data as counter-performance' model, as described by the statement "I agree to data about me being collected and processed, if I can use the respective services free of charge." (numerical values in Table A.2 in Appendix A).

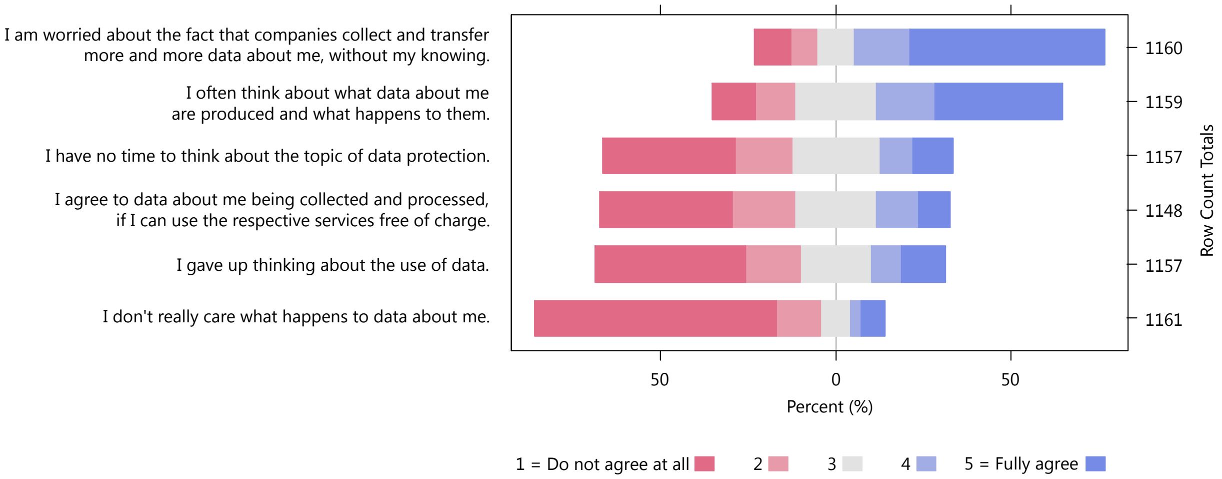


Figure 7.2: Attitudes towards privacy and data protection

Notes: N = 1,331. 170 respondents with no computer and internet use or no answers not shown here. Numerical values of responses (1 to 5) were re-orientated in order to get directions in answering similar to other figures, verbal answering options (Do not agree at all, fully agree) remain the same. Items were read in random order to respondents.

Table 7.2 depicts the percentage of the population that take certain measures or use certain tools to protect their personal data and privacy. Responding to the question "Which of the following measures of data protection have you taken within the last 12 months?", more than 50 percent of the respondents agreed to the statement that they change settings of their browser or that they install apps which are considered more privacy-enhancing. Over 20 percent of the population uses 'privacy-enhancing technologies' (PETs) in the form of internet connections with Virtual Private Networks (VPN) or the Tor browser.

Table 7.2: Individuals taking measures for self-management in data protection

Description of Measures	Percent (%)
I use e-mail programs or e-mail providers that are known for better data protection.	47.5
When registering for internet services, I often do not use my real name.	34.2
I have changed the settings of my browser, i.e. the program for surfing the internet, for better data protection, e.g. by preventing cookies from being set.	58.9
If possible, I install apps on my smartphone or tablet that are considered more privacy-enhancing.	51.6
I regularly use search engines on the internet that are considered relatively privacy-friendly, e.g. DuckDuckgo, Startpage or Ixquick.	17.7
When surfing the internet, I often take measures to obscure my data traces, e.g. VPN connections or the Tor browser.	21.0
I have denied access to my location for certain internet services or apps.	59.5

Notes: N = 1,331. Multiple answers were possible. Items were read in random order to respondents.

Both results on attitudes towards and measures of data protection actually taken may lead to the assumption that the population not just has privacy concerns in an abstract and general way, but is actually taking specific measures and efforts to 'self-protect' itself. Measures taken according to other surveys (European Commission 2016; Statistisches Bundesamt 2016) included changing privacy settings of internet browsers, avoiding certain websites, use of software to prevent adverts to be seen or their online activities from being monitored, measures to control the access to personal information in the internet, restriction of access to own profiles or content on social network websites, or giving no consent to the use of personal data for advertising. However, although the numbers suggested data protection activities of the users, self-management in data protection has some limits, as is illustrated by the example of disabling the installation of cookies in internet browsers. Even if users disabled HTTP cookies, they still can be tracked by so-called 'flash cookies' or 'super cookies' or device fingerprinting (US GAO 2013, p. 23; Article 29 DPWP 2014). Consumers can attempt to prevent them by installing further add-ons to the browser, but this often results in the disadvantage that the browser does not display websites properly or the use of the website is blocked.

7.1.4 Personal value orientation

Personal values refer to what is important to people in their lives and the goals they strive to attain. With regard to the value orientation of the population, Table 7.3 presents the goals describing the personal value, the means of the centred scores (M), and the standard deviations (SD). The centred scores indicate how important the value is for a person in relation to all other values (Schwartz, Breyer and Danner 2015, p. 4f.). As a result of the survey, for the German population, *benevolence, universalism,* and *security* are on the average more important than *power, stimulation,* or *achievement.*

To assess the representativeness of our sample with regard to personal values, we compared the results with the German results of the European Social Survey (ESS) round 6 (Schwartz, Breyer and Danner 2015, p. 18). The ESS is an academically driven cross-national survey that has been conducted across Europe every two years since 2002. The German sample of the ESS consisted of 2,958 participants based on a random probability sampling. Based on the means and standard deviations (SD) provided in the paper (Schwartz, Breyer and Danner 2015, p. 18), we computed effect size *r* to assess differences between our sample and those of the ESS. There were no differences in *self-direction*, *conformity*, *tradition*, and *benevolence* (all $r < 0.02$). Compared to the ESS, the personal values of *universalism* ($r = 0.42$) and *hedonism* ($r = 0.37$) increased and those of *achievement* ($r = 0.26$), *power* ($r = 0.33$), and *stimulation* ($r = 0.57$) decreased moderately. We observed a strong increase in the personal value of *security* ($r = 0.63$). However, this might be an artefact of the survey, as personal values were measured after the 'big data' scenarios. Overall, our results are comparable to those of the ESS.

Table 7.3: Personal value orientation

Values	Goals	N	M	SD
Achievement	Personal success through demonstrating competence according to social standards.	1,315	-0.56	0.95
Benevolence	Preservation and enhancement of the welfare of people with whom one is in frequent personal contact.	1,321	0.90	0.62
Conformity	Restraint of actions, inclinations, and impulses likely to upset or harm others and violate social expectations or norms.	1,292	-0.46	0.93
Hedonism	Pleasure and sensuous gratification for oneself.	1,319	-0.02	0.81
Power	Control or dominance over people and resources.	1,307	-1.28	0.94
Security	Safety, harmony, and stability of society, of relationships, and of oneself.	1,316	0.43	0.83
Self-Direction	Independent thinking and action-choosing, creating, exploring.	1,310	0.39	0.82
Stimulation	Excitement, novelty, and challenge in life.	1,320	-0.66	0.95
Tradition	Respect, commitment, and acceptance of the customs and ideas that traditional culture or religion provide.	1,318	0.00	0.85
Universalism	Understanding, appreciation, tolerance, and protection of the welfare of all people and of nature.	1,313	0.84	0.64

Notes: Value and goals descriptions were adapted from (Schwartz, Breyer and Danner 2015, p. 5f.). Sample size (N), reference means of the centred scores (M), and standard deviations (SD) for the Human Value Scale of the German population are shown. Items were weighted and recoded before analysis.

7.2 Attitudes towards 'big data' practices (RQ1 and RQ2)

To answer research question RQ1 (Can some features of big data practices be identified, which contribute in particular to the sceptical attitude?), the survey results were analysed by counting the frequencies of answers. Regarding RQ2 (Can individuals be differentiated with respect to their sceptical attitude on big data practices?), statistical analyses were computed in order to explore relations to potentially moderating variables.

Previous results of the project, especially the citizens' conferences, suggested a diffuse understanding of the term 'big data'. For this reason, the core of the survey consisted of scenarios of big data practices without using the term 'big data' and describing situations of exemplary big data practices instead. This was supported by the result obtained when asking whether interviewees had heard of the term 'big data' and whether they expected big data to result in more advantages or disadvantages for society in general. 62 percent of the population had not heard of the term 'big data'. The 37 percent of the population, who had heard of the term (N = 498), could be further differentiated in 46 percent, who expected more disadvantages for society and 26 percent expecting more advantages (19 percent answer 'cannot decide', 7 percent 'don't know', 1 percent is not specified).

7.2.1 Assessment of the scenarios (RQ1)

With regard to research question RQ1 (Can some features of big data practices be identified, which contribute in particular to the sceptical attitude?), an assessment of the scenarios 'retail', 'health insurance', 'credit', and 'employment' successively addressed the features differentiation, use of data from the internet, automated decision-making, behavioural adaptations, and protection measures requested. Figure 7.3 summarises the results by showing the means of the response values on agreement or disagreement to statements about features of each of the four scenarios (numerical values in Table A.3 in Appendix A).

One of the main results with regard to RQ1 was that the differences in the survey results for the four scenarios were only minor (some minor exceptions mentioned below). This contradicts the usual assumption that privacy attitudes and concerns are specific for contexts (see Section 6.3.1, description on (4) Attitudes). A possible interpretation for this is that the scenarios describe situations with relative similar consequential decisions that might have implications for the personal self-development and conditions of living. Due to the minor differences between the scenarios, the responses were analysed in a summarizing way with the use of means of the four scenarios (The numbering Item S1 to S23 refers to the summarizing analysis of the scenarios. The respective questions for each scenario are given in the questionnaire in Appendix B).

Differentiations. The scenarios were introduced by brief descriptions of differentiations like price discrimination in the scenario 'retail' with an orientation to generate revenues, managing risks in 'health insurance' and 'credit', and differentiation of wages and working conditions in the scenario 'employment' (see questionnaire in Appendix B). In each scenario, differentiation was based on personal profiles. In the 'retail' scenario, the profile was based on the collection of personal data, in the 'health insurance' scenario on the collection and analysis of body data, e.g. on physical activities recorded by fitness trackers, special apps on smartphones or smartwatches that are connected to the internet, in the 'credit' scenario on the analysis of income, financial circumstances, and payments, i.e. what was bought and paid for, and in the 'employment' scenario on recording and analysing the activities of the employees, e.g. how fast emails were answered, the typing speed, or what was written in emails.

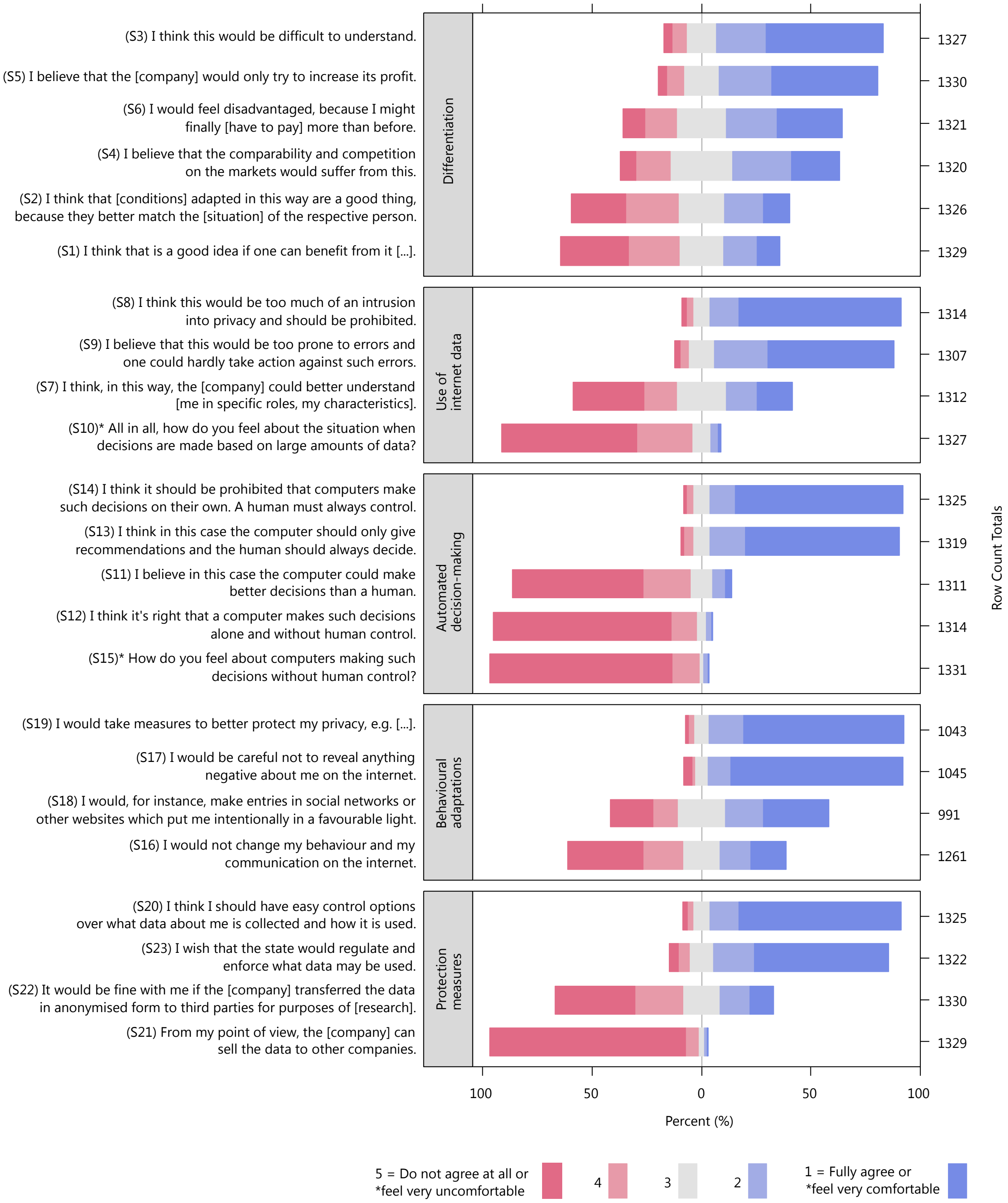


Figure 7.3: Assessments of scenario statements

Notes: N = 1,331. Respondents whose answers cannot be specified are not shown. Chart depicts the frequency of the means of the four scenarios. Means were regrouped before analysis in order to achieve comparability with other results of the study. Items were read in random order to respondents within sections 'Differentiation', 'Use of internet data', 'Automated decision-making', 'Behavioural adaptations', and 'Protection measures'. Items marked with an asterisk (*) have answering options anchored with "5 = feel very uncomfortable" to "1 = feel very comfortable".

Most respondents rejected such differentiations based on the use of large sets of personal data by not (fully) agreeing to statements about possible advantages in the form of receiving benefits, such as regular discounts in retail, favourable rates in insurance, cheaper credits, or being better appraised in employment (Item S1, 53.9 percent of the population with 'disagreement', 25.4 percent 'agreement'). In this Section 7.2.1, the percent of the population is given for 'disagreement' to (or 'uncomfortableness' with) the statements by summarizing the numerical values for the response values 5 = do not agree at all (or feel very unformfortable) and 4, and for 'agreement' to (or 'comfortableness' with) statements by summarizing the numerical values for the response values 2 and 1 = fully agree (or feel very comfortable).

Similar results were obtained for statements saying that conditions adapted in this way would better match the situation or needs of the respective person, such as lower prices for pupils, pensioners, or welfare recipients in retail, insurance rates tailored to the person's individual situation, e.g. a healthy or unhealthy lifestyle in health insurance, creditworthiness or the ability to repay a credit, work experiences and qualification in employment (Item S2, 48.7 percent 'disagreement', 29.5 percent 'agreement'). On the other hand, majorities tended to agree to statements about possible disadvantages, i.e. that it would be difficult to understand (Item S3, 10.1 percent 'disagreement', 75.7 percent 'agreement'), that the company would only try to increase its profit (Item S5, 11.5 percent 'disagreement', 72.1 percent 'agreement'), that they would be disadvantaged by higher prices, worse tariffs or credit terms or worse wages or working conditions (Item S6, 24.3 percent 'disagreement', 52.5 percent 'agreement'), or that the comparability and comparison on markets could decrease (Item S4, 22.5 percent 'disagreement', 48.5 percent 'agreement'). A minor difference between the scenarios is: In the scenario 'employment', interviewees less often agreed with the statement of S4 ("I believe that the comparability and competition on the markets would suffer from this.") than in other scenarios.

Use of internet data. In a next step of the questionnaire, the use of personal data gathered from the internet was added, introduced by the description "... data from the internet, e.g. your communication in social networks and other information found about you on the internet, ..." in order to construct or develop the profile. Respondents were sceptical about possible advantages, such as enhanced understanding of them as customers, insured, borrowers or employees and of their solvency, lifestyle, and risks or performance (Item S7, 46.6 percent 'disagreement', 29.7 percent 'agreement'). A large portion agreed to statements about disadvantages, i.e. the possible intrusion into privacy (Item S8, 5.0 percent 'disagreement', 86.3 percent 'agreement') or that this would be too prone to errors (Item S9, 5.9 percent 'disagreement', 80.5 percent 'agreement'). Respondents showed a very uncomfortable feeling about decisions being made based on large amounts of data (Item S10, 86.8 percent 'uncomfortableness', 4.5 percent 'comfortableness'). Compared to other scenarios, only in scenario 'employment' respondents slightly less often agreed to statement of S7 ("I think, in this way, the [company] could better understand [me in specific roles, my characteristics].").

Automated decision-making. Statements about automated decision-making done by computers produced even more unambiguous results in the form of rejecting that the computer should make such decision alone and without human control (Item S12, 91.5 percent 'disagreement', 2.9 percent ‘agreement’), or that the computer makes better decisions than a human (Item S11, 79.7 percent ‘disagreement’, 8.4 percent ‘agreement’). Instead, the majority of respondents agreed to the statements that computers should only give recommendations and a human should always decide (Item S13, 5.3 percent ‘disagreement’, 85.6 percent ‘agreement’), and even that it should be prohibited that computers make such decisions alone (Item S14, 4.0 percent ‘disagreement’, 87.5 percent ‘agreement’). A large portion of respondents felt uncomfortable about computers making such decisions without human control (Item S15, 95.5 percent ‘uncomfortableness’, 2.1 percent ‘comfortableness’).

Behavioural adaptations. Against the backdrop of the scenario descriptions, interviewees were asked for statements on possible behavioural adaptations. The results suggested agreements statements about taking measures for privacy protection, “... e.g. using only social networks or search engines that are known for better privacy protection” (Item S19, 2.9 percent ‘disagreement’, 69.7 percent ‘agreement’) as well as to being careful not to reveal anything negative on the internet (Item S17, 3.9 percent ‘disagreement’, 69.9 percent ‘agreement’), which might be interpreted as a kind of ‘self-restriction’. The statement directly addressing a change of behaviour and communication on the internet produced ambiguous results (Items S16, 49.8 percent ‘disagreement’, 28.6 percent ‘agreement’), although a considerable portion of 35.1 percent of the population agreed to the option of making entries in online social networks or other websites which deliberately throw a positive light on them (Item S18, summarized to 22.8 percent ‘disagreement’, 35.1 percent ‘agreement’). Those results suggested a certain level of ‘chilling effects’ as a reaction to the use of such kind of data. The differences between scenarios are only minor: In the scenarios ‘employment’ and ‘credit’, interviewees would adapt their behaviour as described in Item S18 (“I would, for instance, make entries in social networks or other websites which put me intentionally in a favourable light.”) slightly more than in other scenarios.

Protection measures. Furthermore, interviewees were asked for required or allowed measures of data protection as an immediate reaction to the scenario descriptions. The results revealed a clear agreement to easy control options for individuals (Item S20, 4.5 percent ‘disagreement’, 86.9 percent ‘agreement’) and to state interventions to regulate and enforce what data about individuals may be used (Item S23, 9.0 percent ‘disagreement’, 79.2 percent ‘agreement’). Results were also a clear disagreement to selling personal data to other companies (Item S21, 95.3 percent ‘disagreement’, 1.7 percent ‘agreement’) or, in majority but more varied, transferring anonymised data to third parties for research purposes (Item S22, 58.5 percent ‘disagreement’, 24.4 percent ‘agreement’). The latter two results also indicated a preference of the population to the adherence to the principle of purpose limitation (see also Section 7.3.2). Some minor differences between the scenarios exist for agreeing to data transfer to third parties (Item S22): respondents slightly agree less to the statement in the scenarios ‘retail’ and ‘employment’.

7.2.2 Potential moderators (RQ2)

With regard to research question RQ2 for possible differences between attitudes on big data practices, the study used measures of associations indicating the levels of dependence between demographic variables, personal value orientations as well as variables on computer and internet use and data protection, on the one hand, and variables of selected scenario statements on big data practices, on the other. Items S1, S2, S4, S6, S7, S16, S18, and S22 from Figure 7.3 were selected for further analysis due to requirements on the necessary dispersion. Due to the large sample size, already small effects reached statistical significance. To assess the practical significance, we considered effect sizes. For nominally scaled variables, we computed chi square (χ^2) tests and reported Cramérs' V values; if one of the variables was interval-scaled, we computed Analyses of Variance (ANOVA) and reported partial eta squared ($\eta_p{}^2$) values. For interpretation, we followed the conventions by Cohen (1988). The χ^2-test for associations was made between variables of demographics, frequency of computer and internet use, knowledge about computers and the internet, self-management in data protection, on the one hand, and attitudes towards big data practices, on the other, showing the chi square (χ^2) values, Cramérs' V (V), degree of freedom (df), and significance (p). Cramérs' V values indicate that all observed effects were only weak ($V < 0.3$) and, thus, negligible (weak effects in bold in Table A.4 in Appendix A). The analysis of variance (ANOVA) addressed distinctions between the level of agreement to scenario statements and the personal value orientations. The presented partial eta squared ($\eta_p{}^2$) values, as measures of effect size or strength of relationship between variables, indicate no ($\eta_p{}^2 < 0.01$) or only weak effect sizes ($0.01 < \eta_p{}^2 < 0.06$) (weak effects in bold in Table A.5 in Appendix A). Both analyses addressing RQ2 revealed that individuals cannot be differentiated along the variables taken into account in this study.

7.3 Attitudes towards the institutional framework of privacy and data protection (RQ3 and RQ4)

After questions about big data practices, interviewees answered questions about their opinions on and knowledge about responsibilities, measures, individual rights of data subjects, and legal instruments of privacy and data protection to tackle research questions RQ3 (Against the backdrop of exemplary big data practices, what are the opinions of the population with regard to the institutional privacy and data protection framework or other measures required?) and RQ4 (Can individuals be differentiated with respect to their opinions on the institutional framework?). RQ3 was addressed by counting frequencies, while statistical analyses were computed to deal with RQ4. The results are structured along the considered principles, instruments and rights of privacy and data protection regulations, i.e. privacy policies, purpose limitation, and special individuals' rights and further measures of data protection demanded.

7.3.1 Reading and understanding of privacy policies

As depicted in Figure 7.4 with regard to the informed consent approach, only 9.5 percent of the population 'always' read the privacy policies at least partly and 17.2 percent did this 'often' (26.3 percent 'sometimes', 25.3 percent 'rarely', 18.9 'never', 2.9 percent 'not specified'). Of those respondents, who read privacy policies at least partly (and at least rarely), only 5.9 percent felt to have ‘always’ understood them largely and 15.6 percent ‘often’ (28.4 percent ‘sometimes’, 24.7 percent ‘rarely’, 3.2 percent ‘never’, 3.3 percent ‘not specified’).

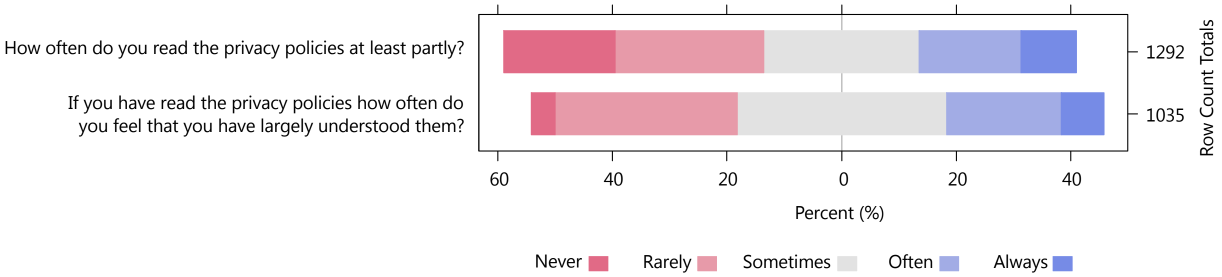


Figure 7.4: Reading and understanding of privacy policies

Notes: N = 1,331. Respondents whose answers cannot be specified are not shown. 251 respondents (or 18.9 percent), who stated never to read privacy policies, are not shown in the Item about understanding privacy policies. Numerical values of responses (1 to 5) were re-orientated in order to get directions in answering similar to other figures, verbal answering options remain the same.

Further analysis by a χ^2 test for associations revealed significant relations between the frequency of reading privacy policies and gender, age, education level, frequency of computer and internet use, and level of privacy self-management (shown in Table A.6 in Appendix A). For the understanding of privacy policies, the impact of age, education, frequency of computer and internet use, knowledge about computers, the level of privacy self-management, and of whether respondents heard of the term ‘big data’ was significant. However, the effect sizes were only weak (Cramers’ V < 0.3) and, thus, negligible (weak effect sizes in bold in Table A.6). Table A.7 in Appendix A depicts that effect sizes calculated by an Analysis of Variance (ANOVA), which were also weak for relationships between reading and understanding of privacy policies, on the one hand, and particular personal value orientations, on the other ($\eta_p^2 < 0.06$) (weak effect sizes in bold in Table A.7). Both analyses to answer RQ4 did not identify any variable of those considered to differentiate individuals with respect to reading and understanding privacy policies.

Regarding the question “What measures would you like to see introduced to support you with privacy policies?”, respondents agreed by majority to the proposed measures “A simple and clear language that everyone can understand” (91.5 percent of the population), “Data and consumer protection organisations should examine the privacy policies and take action against misuse” (84.9 percent), “Privacy policies should be examined by governmental agencies, and misuse should be punished.” (81.8 percent), and “Simple symbols that inform about the types of data use” (73.5 percent). This indicates a preference not for a single measure, but for a mixture of them (N = 1,331; Items read in random order to respondents; ‘yes’ or ‘no’ answering options). Further suggestions by respondents noted by the interviewers included demands for shorter privacy policies (N = 20), improvements of formulations and language (N = 13), or enhancing the legibility and comprehensibility, e.g. larger letters or symbols (N = 10), among other things.

7.3.2 Purpose limitations and trust

Introduced by the sentence “Assuming you consented to a company’s privacy policies and data processing purposes described therein”, respondents agreed or disagreed to statements describing their thoughts about current data processing and compliance with the provision of *purpose limitation* by data controllers or companies. Results which are summarised in Figure 7.5 suggested that the population tends to distrust the companies’ behaviour of obeying to the provisions of purpose limitation and the data processing practices described in their privacy policies (numerical values in Table A.8 in Appendix A).

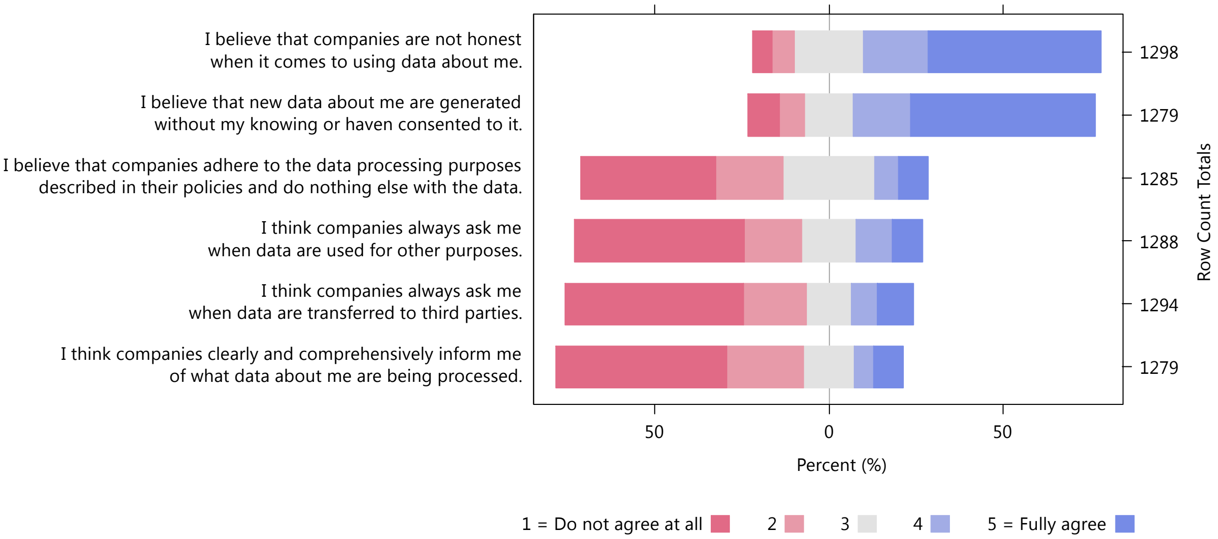


Figure 7.5: Attitudes towards purpose limitation

Notes: N = 1,331. Respondents whose answers cannot be specified are not shown here. Items were read in random order to respondents. Numerical values of responses (1 to 5) were re-orientated in order to get directions in answering similar to other figures. Verbal answering options (Do not agree at all, fully agree) remain the same.

Also for attitudes towards purpose limitations and trust in data controllers, further analyses were conducted by computing χ^2-tests for the relationship to potential moderators (Table A.9 in Appendix A) and Analyses of Variance (ANOVA) for the relation to personal value orientations (Table A.10 in Appendix A). They only revealed weak effect sizes (in bold in both tables). Among the moderating variables to address research question RQ4, there was no variable along which individuals could be differentiated.

7.3.3 Individuals’ rights and demands on the institutional framework

As shown in Table 7.4, nearly half of the population (48.8 percent) heard of the right of data subjects to ask a data controller for information about personal data processed, termed as ‘right to access’ in the GDPR. The questions for the use of the rights to ask for information or to request correction or erasure were only asked to those who knew the right to ask for information. Only 11.5 percent of the population answered to have used the right to ask for information about personal data and only 6.5 percent of the population answered to have used the right to request for corrections or erasure of personal data.

Table 7.4: Knowledge and use of individuals' rights

	Percent (%) of population			
Description of item	**Do not know the right**	**Yes**	**No**	**Not specified**
Have you ever heard that you have a right to ask a company or an authority for information about the data they process about you?		48.4	51.1	0.5
Have you ever used this option and asked a company or an authority for information about what data they process about you?	51.1	11.5	37.0	0.4
Have you ever heard that you have a right to request correction of incorrect data or erasure of certain data about you?	51.1	40.5	8.1	0.3
Have you ever used this option and requested correction or erasure of data about you?	59.2	6.5	33.9	0.4

Notes: N = 1,331. Respondents who never heard of the right to ask for information and to request corrections or erasure are skipped in the questions on the use of these rights.

Further analysis of relations between the knowledge and use of the rights of data subjects, on the one hand, and potential moderators (χ^2-tests, results in Table A.11 in Appendix A) or personal value orientations (ANOVA, results in Table A.12 in Appendix A), on the other, showed only weak effect sizes (in bold in both tables). With regard to RQ4, the analyses showed that individuals cannot be differentiated along the variables considered.

Table 7.5 depicts attitudes towards responsibilities and demanded data and privacy protection measures that were agreed or disagreed to against the backdrop of previously treated 'big data' practices. A relatively large portion considered the individual to be solely responsible for data protection. This contradicts the high agreements to statements on intensified governmental and legal interventions or measures of organisations for consumer and data protection. Large demands for education and information, either as learning in general or as school education, can be seen to be relatively compatible with it.

Also for demands on the institutional privacy and data protection framework, further analyses discovered only weak and, thus, negligible effect sizes for the relationships between the demands, on the one hand, and either the potential moderators (χ^2-tests, results in Table A.13 in Appendix A, weak effects in bold) or the personal value orientations (ANOVA, results in Table A.14 in Appendix A, weak effects in bold), on the other.

Table 7.5: Demanded measures for data and privacy protection

Description of item	Percent (%)
Everyone is solely responsible for protecting their data.	54.1
I know whom to contact in order to enforce my data protection rights.	31.8
I generally want better information and education about the opportunities and risks of data processing and how to deal with them.	84.6
I would like to learn much more about computers, the internet, and data protection.	63.9
I would like to see children and young people being taught about the opportunities and risks of data processing already in school.	97.7
I think it would be good if consumer and data protection organisations took more action against misuse of data.	98.0
The existing data protection laws should be better enforced.	94.5
There should be more government investigations to ensure that as few data as possible are collected about me.	89.9
The government should regulate by law and ensure by necessary precautions that I always know what data about me are processed.	90.5
The government should impose harsher penalties for misuses of personal data.	91.6
The international transfer of data should be better controlled and regulated.	94.4

Notes: N = 1,331. Percent of respondents agreeing with 'yes' to the statements is shown. Multiple answers possible. Items were read in random order to respondents, except last item.

8 Discussion

The study is based on the observation that the general public has a sceptical view on big data applications. The aim was to gain insights into the factors influencing it. The survey showed relatively uniform attitudes towards 'big data' practices and influencing factors, in contrast to the usual context specificity of privacy issues, concerns or attitudes. Overall, the results of the study revealed that the German population was sceptical about 'big data' practices irrespective of the scenario, i.e. scenarios of big data-based price discrimination in retail, differentiated tariffs in health insurance, credit scoring, and differentiated wages and working conditions in employment. Of the considered features of big data practices, the use of data from the internet (e.g., from online social networking sites), automated decision-making by computers in the situations described, and the selling of the data to other companies were unambiguously rejected. Uniform results were also obtained for the statement that big data practices were difficult to understand, for the suspicion that companies would only try to increase their profits, and for a demand for easy control options and regulations by the state. Additionally, the results were uniform for statements that describe that respondents would take measures to protect their privacy or would be careful not to reveal anything negative when data from the internet would be used for big data-based differentiation. Especially these findings on potential reactions to big data practices as a kind of self-restriction contradict the intentions of the fundamental right of informational self-determination to ensure a free and autonomous development of personality through individual reflexive self-determination, as well as self-presentation, free speech and opinion to build a democratic society.

Among the items of big data practices seen relatively varied, but tentatively rejected, were those about possible advantages or benefits of big data-based differentiations for the affected persons, i.e. to enable a better matching of the situation and needs of respective persons, if the use of data from the internet would increase the understandings about the affected persons, or with regard to the transfer of data in anonymised form for purposes of research. We can conclude that the majority of the population did not see benefits of big data applications.

Responses by the population also varied as to whether comparability and competition on markets would suffer, whether respondents would possibly react to the use of data from the internet or whether they would deliberately make entries in social networks that would throw a positive light on them. Even for these items indicating a dispersion of answers, further analyses discovered only weak effects by the potential moderators and personal value orientations. Hence, the answer of the research question relating to the factors influencing the attitudes was that no variable investigated in the survey can be considered to be very much responsible for the divergence in attitudes towards these features of big data practices, neither age, nor gender, income level, educational level, instances of computer literacy, or personal value orientations. With regard to behavioural adaptations, the majority of the population would react on the described big data practices, in particular, by taking measures to better protect the privacy or by being careful not to reveal anything negative about them on the internet. A considerable portion of 35.1 percent even would make entries in online social networks or other websites which deliberately throw a positive light on them.

Results also confirmed previous empirical findings and arguments that privacy policies mostly were not read and less frequently understood, that the majority of the population thinks that companies do not adhere to the principle of purpose limitation, and that a majority of the population does not know and use the rights to request information about the processing of personal data or to correct or erase certain data. These results point to challenges posed by applications of big data for principles and instruments of the institutional framework questioning the adequacy of its existing elements. Further analyses to investigate whether certain groups of the population can be differentiated with regard to their attitudes towards the institutional privacy and data protection framework also revealed only weak and, thus, negligible effects of the above mentioned variables. This is the result for the knowledge and use of its principles and instruments, i.e. privacy policies, purpose limitation, individuals' rights, and demands for further data protection measures. Among the policy options most often agreed to by respondents are measures against data misuse that should be taken by organisations of consumer and data protection, educational measures, a better enforcement of existing data protection laws, and a better control and regulation of the international transfer of data. Although the responses were given under the impression of selected big data scenarios, the results suggested, in general, a considerable reliance of the population on governmental measures and interventions confirming previous studies.

9 Limitations of the study and further research

The study has some limitations that have to be taken into account when assessing the results of the survey and that point to further research. The study has an explorative character providing only initial indications of potential relationships among moderating variables and attitudes towards selected big data practices and data protection regulations. Next steps of research could be developing models and further contributions to develop and enrich the understanding of attitudes towards data processing and privacy that take explicitly into account the specific features of big data practices, such as the increased opacity of data uses, transfers, and aggregations and the automation of inferences and decision-making.

The survey focuses on examples of big data practices with personal data, direct consequences for individuals, and mainly individual concerns about it. Other big data practices with non-personal data or with indirect benefits for the population are not considered in this study, such as big data applications in scientific research, industrial manufacturing, business-to-business trade or production relations, which could increase the efficiency of the economy in general or the overall stock of knowledge. The same holds for big data applications by governments, such as for national security and surveillance, policing or behavioural steering ('nudging'), which are not considered here and deserve dedicated research. Population's attitudes towards the indirect benefits and overall welfare effects of big data as well as risks for a functioning society, such as democratic processes or the roles of journalism and the media, could be investigated in further studies. Furthermore, this study focused on potential consequences of big data practices for individuals. Big data-based treatments of groups, which might be opaque for the single individual and potentially circumvent the legal provisions for the processing of personal data, can be subject of further research as well as options to handle such privacy risks.

Questions about privacy and data protection regulations, but also on whether companies obey to them were asked deliberately after treating big data practices. The explorative results have to be assessed in view of the fact that respondents answered under the impression of the scenarios of big data practices (two for each subset) describing potential implications for their personal self-development. Further research might explore in more detail and from other perspectives the balancing of perceived risks for fundamental values and rights, on the one hand, and the population's attitudes towards concrete approaches, individual efforts, required activities, or overall costs of measures of privacy and data protection, on the other.

Further research avenues might lead to investigations of the capabilities of individuals of recognising, assessing, and handling individual benefits and other consequences and risks of data processing by those data controllers applying big data technologies to which they have given consent or that are beyond their (potential) awareness. This might range from activities of data brokers to the development of tracking and analyses of online behaviour, to monitoring within the internet of things, electronic payment systems, or applications of blockchain technologies. Although the survey at hand has addressed roles, capabilities, activities, and boundaries of individuals relating to protection against privacy risks, much more attention on these topics seems to be required. Research might be dedicated to necessary capabilities of and measures to enable individuals to have knowledge about the whole range of factors of big data-based decisions about them and the processes of decision-making as well as to the consequences for the personal development and dignity and the actual harms of privacy issues. Further (empirical) research could cover behavioural reactions to perceived privacy issues, the ‘chilling effects’, and the consequences of a loss of trust and implication for social goals, such as the free development of personality, free speech and democracy, rights to associations, and fair and competitive markets. Ultimately, this research would deliver the knowledge base for the further realization of fundamental rights such as the informational self-determination in more data-intensive contexts.

Data availability

The accompanying data set of the survey is available as open access file at the KITopen repository:
https://doi.org/10.5445/IR/1000087986 or
https://publikationen.bibliothek.kit.edu/1000087986

Acknowledgements

The authors thank Andreas Czech, Oliver Raabe, Oliver Siemoneit, Maurice Niehoff, Daniel Frank, Reinhard Heil, Maike Schröder, Verena Dorner, Tim Bornkessel, and Christina Merz for comments and support.

Funding

The survey is part of the project "Assessing Big Data" (ABIDA) that is partly funded by the Federal Ministry of Education and Research, Germany (Grant No. 01IS15016A-F). CO is also funded within the institutional funding of the Helmholtz Association of German Research Centers and AS receives funding within the EU FP7 project Prosperity4All (grant agreement no. 610510).

Authors contributions

Conceptualization: CO, AS.
Data curation: AS, CO.
Formal analysis: AS, CO.
Funding acquisition: CO (among other project colleagues).
Investigation: CO, AS (including instructing and supervising survey company).
Methodology: AS, CO.
Project administration: CO.
Writing - original draft: CO, AS.
Writing - review and editing: CO, AS.

References

Acquisti, Alessandro; Brandimarte, Laura; Loewenstein, George (2015): Privacy and human behavior in the age of information; in: Science, Vol. 347, Issue 6221, pp. 509-514.

Acquisti, Alessandro; Taylor, Curtis; Wagman, Liad (2016): The Economics of Privacy; in: Journal of Economic Literature, Vol. 54, Issue 2, pp. 442-492.

Agrawal, Ajay; Gans, Joshua; Goldfarb, Avi (2016): The Simple Economics of Machine Intelligence; in: Harvard Business Review, Vol. 17, Issue Nov., pp. 2-5.

Albers, Marion (2017): Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsvorschriften und Rechtspositionen, in: Friedewald, Michael; Lamla, Jörn; Roßnagel, Alexander (eds.): Informationelle Selbstbestimmung im digitalen Wandel, Wiesbaden: Springer, pp. 11-35.

Angrave, David; Charlwood, Andy; Kirkpatrick, Ian; Lawrence, Mark; Stuart, Mark (2016): HR and analytics: why HR is set to fail the big data challenge; in: Human Resource Management Journal, Vol. 26, Issue 1, pp. 1-11.

Arentz, Christine; Rehm, Rebekka (2016): Behavior-based Tariffs in Health Insurance - Compatibility with the German System; Cologne: Otto Wolff Institut für Wirtschaftsordnung.

Article 29 DPWP (2014): Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting; Brussels: Article 29 Data Protection Working Party (Article 29 DPWP).

Article 29 DPWP (2018): Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679; Adopted in 2017, revised in 2018; Brussels: Article 29 Data Protection Working Party (Article 29 DPWP).

Barocas, Solon; Nissenbaum, Helen (2014): Big Data's End Run around Anonymity and Consent, in: Lane, Julia; Stodden, Victoria; Bender, Stefan; Nissenbaum, Helen (eds.): Privacy, Big Data, and the Public Good. Frameworks for Engagement, New York: Cambridge University Press, pp. 44-75.

Barocas, Solon; Selbst, Andrew D. (2016): Big data's disparate impact; in: California Law Review, Vol. 104, pp. 671-732.

Barton, Dominic; Court, David (2012): Making advanced analytics work for you; in: Harvard Business Review, Vol. 90, Issue 10, pp. 78-83.

Baruh, Lemi (2007): Read at your own risk: shrinkage of privacy and interactive media; in: New Media & Society, Vol. 9, Issue 2, pp. 187-211.

Baruh, Lemi; Popescu, Mihaela (2015): Big data analytics and the limits of privacy self-management; in: New Media & Society, Vol. 19, Issue 4, pp. 579-596.

BDSG (2017): Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 10 Absatz 2 des Gesetzes vom 31. Oktober 2017 (BGBl. I S. 3618) geändert worden ist; in: Bundesgesetzblatt, Issue 31.10.2017.

Bélanger, France; Crossler, Robert E. (2011): Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems; in: MIS Quarterly: Management Information Systems, Vol. 35, Issue 4, pp. 1017-1041.

Bitter, Philip; Uphues, Steffen (2017): Big Data und die Versicherungsgemeinschaft - "Entsolidarisierung" durch Digitalisierung?; ABIDA-Dossier, Münster: Westfälische Wilhelms-Universität Münster, Institut für Informations-, Telekommunikations- und Medienrecht.

boyd, Danah; Crawford, Kate (2012): Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon; in: Information, Communication & Society, Vol. 15, Issue 5, pp. 662-679.

Braun, Stefan (2017): Verbrauchereinstellungen und Erwartungen zu algorithmenbasierten Entscheidungsprozessen. Umfrage im Auftrag des Verbraucherzentrale Bundesverband e.V.; Berlin: Civey GmbH.

Burdon, Mark; Harpur, Paul (2014): Re-conceptualising privacy and discrimination in an age of talent analytics; in: University of New South Wales Law Journal, Vol. 37, Issue 2, pp. 679-712.

BVerfG (1983): BVerfGE 65, 1; Urteil vom 15. Dezember 1983, Az. 1 BvR 209/83 u.a. (Volkszählungsurteil); Karlsruhe: Bundesverfassungsgericht (BVerfG).

Carmichael, Laura; Stalla-Bourdillon, Sophie; Staab, Steffen (2016): Data mining and automated discrimination: A mixed legal/technical perspective; in: IEEE Intelligent Systems, Vol. 31, Issue 6, pp. 51-55.

Cate, Fred H.; Mayer-Schönberger, Viktor (2013): Notice and consent in a world of Big Data; in: International Data Privacy Law, Vol. 3, Issue 2, pp. 67-73.

Chamorro-Premuzic, Tomas; Akhtar, Reece; Winsborough, Dave; Sherman, Ryne A. (2017): The datafication of talent: how technology is advancing the science of human potential at work; in: Current Opinion in Behavioral Sciences, Vol. 18, Issue Dec., pp. 13-16.

Chamorro-Premuzic, Tomas; Winsborough, Dave; Sherman, Ryne A.; Hogan, Robert (2016): New Talent Signals: Shiny New Objects or a Brave New World?; in: Industrial and Organizational Psychology, Vol. 9, Issue 3, pp. 621-640.

Charter of Rights (2012): Charter of Fundamental Rights of the European Union (2012/C 326/02); in: Official Journal of the European Union, Issue C 326, 26.10.2012, pp. 391-407.

Chen, Min; Mao, Shiwen; Liu, Yunhao (2014): Big Data: A Survey; in: Mobile Networks and Applications, Vol. 19, Issue 2, pp. 171-209.

Christl, Wolfie (2017): Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions; Vienna: Cracked Labs.

Christl, Wolfie; Spiekermann, Sarah (2016): Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy, Wien: Facultas Verlags- und Buchhandels AG.

Citron, Danielle Keats (2008): Technological Due Process; in: Washington University Law Review, Vol. 85, Issue 6, pp. 1249-1313.

Citron, Danielle Keats; Pasquale, Frank (2014): The scored society: due process for automated predictions; in: Washington Law Review, Vol. 89, Issue 1, pp. 101-133.

Cohen, Jacob (1988): Statistical Power Analysis for the Behavioral Sciences, Hillsdale: Lawrence Erlbaum Associates.

Constantiou, Ioanna D.; Kallinikos, Jannis (2015): New games, new rules: big data and the changing context of strategy; in: Journal of Information Technology, Vol. 30, Issue 1, pp. 44-57.

Cranor, Lorrie Faith; Hoke, Candice; Leon, Pedro Giovanni; Au, Alyssa (2014): Are They Worth Reading? An In-Depth Analysis of Online Advertising Companies' Privacy Policies; in: I/S: A Journal of Law and Policy for the Information Society, Vol. 11, Issue 2, pp. 325-404.

Das, Sauvik; Kramer, Adam D. I. (2013): Self-Censorship on Facebook, at: Proceedings of the Seventh International AAAI Conference on Weblogs and Social Media (ICWSM); published by Association for the Advancement of Artificial Intelligence.

Davenport, Thomas H.; Barth, Paul; Bean, Randy (2012): How big data is different; in: MIT Sloan Management Review, Vol. 54, Issue 1, pp. 22-24.

de Montjoye, Yves-Alexandre; Radaelli, Laura; Singh, Vivek Kumar; Pentland, Alex "Sandy" (2015): Unique in the shopping mall: On the reidentifiability of credit card metadata; in: Science, Vol. 347, Issue 6221, pp. 536-539.

Deutscher Ethikrat (2017): Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung Stellungnahme; Berlin: Deutscher Ethikrat.

Drake, John R.; Hall, Dianne; Becton, J. Bret; Posey, Clay (2016): Job applicants' information privacy protection responses: Using social media for candidate screening; in: AIS Transactions on Human-Computer Interaction, Vol. 8, Issue 4, pp. 160-184.

Dzida, Boris (2017): Big Data im Arbeitsrecht; in: Neue Zeitschrift für Arbeitsrecht (NZA), Vol. 34, Issue 9, pp. 541-546.

EDPS (2017): Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content; Brussels: European Data Protection Supervisor (EDPS).

Ekbia, Hamid; Mattioli, Michael; Kouper, Inna; Arave, G.; Ghazinejad, Ali; Bowman, Timothy; Suri, Venkata Ratandeep; Tsou, Andrew; Weingart, Scott; Sugimoto, Cassidy R. (2015): Big data, bigger dilemmas: A critical review; in: Journal of the Association for Information Science and Technology, Vol. 66, Issue 8, pp. 1523-1545.

Eschholz, Stefanie (2017): Big Data-Scoring unter dem Einfluss der Datenschutz-Grundverordnung; in: Datenschutz und Datensicherheit - DuD, Vol. 41, Issue 3, pp. 180-185.

European Commission (2015): Data Protection. Special Eurobarometer 431, Report. Survey conducted by TNS Opinion & Social at the request of Directorate-General for Justice and Consumers (DG JUST); Brussels: European Commission, Directorate-General for Communication.

European Commission (2016): e-Privacy. Flash Eurobarometer 443, Report. Survey conducted by TNS Political & Social at the request of the European Commission, Directorate-General for Communications Networks, Content & Technology (DG CONNECT); Brussels: European Commission, Directorate-General for Communication.

Eurostat (2016): Big data analysis; Luxembourg: European Commission, Eurostat2017-09-30.

Ezrachi, Ariel; Stucke, Maurice E. (2016): Virtual Competition. The Promise and Perils of the Algorithm-Driven Economy, Cambridge, London: Harvard University Press.

Ferretti, Federico (2017): Not-So-Big and Big Credit Data Between Traditional Consumer Finance, FinTechs, and the Banking Union: Old and New Challenges in an Enduring EU Policy and Legal Conundrum; in: Global Jurist, pp. 1-41.

Fischer, Sarah; Petersen, Thomas (2018): Was Deutschland über Algorithmen weiß und denkt. Ergebnisse einer repräsentativen Bevölkerungsumfrage; Gütersloh: Bertelsmann Stiftung.

Fosso Wamba, Samuel; Akter, Shahriar; Edwards, Andrew; Chopin, Geoffrey; Gnanzou, Denis (2015): How 'big data' can make big impact: Findings from a systematic review and a longitudinal case study; in: International Journal of Production Economics, Vol. 165, Issue Supplement C, pp. 234-246.

FTC (2014): Data Brokers. A Call for Transparency and Accountability; Washington, D.C.: Federal Trade Commission (FTC).

FTC (2016): Big Data. A Tool for Inclusion or Exclusion?; Washington, D.C.: Federal Trade Commission (FTC).

GDPR (2016): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance); in: Official Journal of the European Union, Issue L 119, 4.5.2016, pp. 1-88.

Goldfarb, Avi; Tucker, Catherine (2017): Digital Economics; NBER Working Paper 23684, Cambridge, MA: National Bureau of Economic Research.

Gonçalves, Maria Eduarda (2017): The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward; in: Information & Communications Technology Law, Vol. 26, Issue 2, pp. 90-115.

Grunwald, Armin (2009): Technology Assessment: Concepts and Methods, in: Meijers, Anthonie (ed.): Handbook of the Philosophy of Science, Volume 9: Philosophy of Technology and Engineering Sciences, Amsterdam et al.: Elsevier/North Holland, pp. 1103-1146.

Hallinan, Dara; Friedewald, Michael; McCarthy, Paul (2012): Citizens' perceptions of data protection and privacy in Europe; in: Computer Law & Security Review, Vol. 28, Issue 3, pp. 263-272.

Hildebrandt, Mireille; Koops, Bert-Jaap (2010): The Challenges of Ambient Law and Legal Protection in the Profiling Era; in: The Modern Law Review, Vol. 73, Issue 3, pp. 428-460.

Horvitz, Eric; Mulligan, Deirdre (2015): Data, privacy, and the greater good; in: Science, Vol. 349, Issue 6245, pp. 253-255.

Hügle, Anika (2017): Big Data - Lösung oder Problem? Dokumentation und Analyse der Bürgerkonferenzen; Bericht des Projekts ABIDA - Assessing Big Data; Karlsruhe: Karlsruher Institut für Technologie, Institut für Technikfolgenabschätzung und Systemanalyse.

Hurley, Mikella; Adebayo, Julius (2016): Credit Scoring in the Era of Big Data; in: Yale Journal of Law & Technology, Vol. 18, Issue 1, pp. 148-216.

Jarchow, Thomas; Estermann, Beat (2015): Big Data: Chancen, Risiken und Handlungsbedarf des Bundes. Ergebnisse einer Studie im Auftrag des Bundesamts für Kommunikation; Bern: Berner Fachhochschule, E-Government-Institut.

Kallinikos, Jannis; Constantiou, Ioanna D. (2015): Big data revisited: a rejoinder; in: Journal of Information Technology, Vol. 30, Issue 1, pp. 70-74.

Kettner, Sara Elisa; Thorun, Christian; Vetter, Max (2018): Wege zur besseren Informiertheit. Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz; Berlin: ConPolicy GmbH, Institut für Verbraucherpolitik.

Kitchin, Rob (2014): The Data Revolution. Big Data, Open Data, Data Infrastructures and Their Consequences, London et al.: Sage.

Kitchin, Rob; McArdle, Gavin (2016): What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets; in: Big Data & Society, Vol. 3, Issue 1, pp. 1-10.

Kokolakis, Spyros (2017): Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon; in: Computers & Security, Vol. 64, Issue Jan., pp. 122-134.

Kolany-Raiser, Barbara; Heil, Reinhard; Orwat, Carsten; Hoeren, Thomas (eds.) (2018): Big Data und Gesellschaft. Eine multidisziplinäre Annäherung, Wiesbaden: Springer VS.

König, René (2016): Big Data, Big Problems? Bericht zum Experten-Workshop des Projektes Assessing Big Data; in: Technikfolgenabschätzung - Theorie und Praxis, Vol. 25, Issue 2, pp. 101-103.

Laney, Doug (2001): 3D Data Management: Controlling Data Volume, Velocity, and Variety; Application Delivery Strategies, Stamford: Meta Group; available at: blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf, last access at: 2017-09-11.

Lang, Caroline; Barton, Hannah (2015): Just untag it: Exploring the management of undesirable Facebook photos; in: Computers in Human Behavior, Vol. 43, Issue Feb., pp. 147-155.

Lepri, Bruno; Oliver, Nuria; Letouzé, Emmanuel; Pentland, Alex; Vinck, Patrick (2017): Fair, Transparent, and Accountable Algorithmic Decision-making Processes; in: Philosophy & Technology, Vol. Online first.

Lukaszewski, Kimberly M.; Stone, Diana L.; Johnson, Richard D. (2016): Impact of human resource information system policies on privacy; in: AIS Transactions on Human-Computer Interaction, Vol. 8, Issue 2, pp. 58-73.

Marder, Ben; Joinson, Adam; Shankar, Avi; Houghton, David (2016): The extended 'chilling' effect of Facebook: The cold reality of ubiquitous social networking; in: Computers in Human Behavior, Vol. 60, Issue Jul., pp. 582-592.

Marler, Janet H.; Boudreau, John W. (2017): An evidence-based review of HR Analytics; in: The International Journal of Human Resource Management, Vol. 28, Issue 1, pp. 3-26.

Marthews, Alex; Tucker, Catherine E. (2017): Government Surveillance and Internet Search Behavior; Cambridge, MA: Digital Fourth and MIT Sloan School of Management.

Martin, Kirsten (2013): Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online; in: First Monday, Vol. 18, Issue 12 (online article) http://www.firstmonday.dk/ojs/index.php/fm/article/view/4838/3802.

Martin, Kirsten (2015): Privacy notices as tabula rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online; in: Journal of Public Policy & Marketing, Vol. 34, Issue 2, pp. 210-227.

Martin, Kirsten (2016): Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online; in: The Journal of Legal Studies, Vol. 45, Issue S2, pp. S191-S215.

Martin, Kirsten; Nissenbaum, Helen (2016): Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables; in: Columbia Science and Technology Law Review, Vol. 18, Issue Fall, pp. 176-218.

Martini, Mario (2017): Algorithmen als Herausforderung für die Rechtsordnung; in: Juristenzeitung, Vol. 72, Issue 21, pp. 1017-1025.

Matz, S. C.; Kosinski, M.; Nave, G.; Stillwell, D. J. (2017): Psychological targeting as an effective approach to digital mass persuasion; in: Proceedings of the National Academy of Sciences (PNAS), Vol. 114, Issue 48, pp. 12714-12719.

Matz, Sandra C.; Netzer, Oded (2017): Using Big Data as a window into consumers' psychology; in: Current Opinion in Behavioral Sciences, Vol. 18, Issue Dec., pp. 7-12.

McDonald, Aleecia M.; Cranor, Lorrie Faith (2008a): The cost of reading privacy policies; in: I/S: A Journal of Law and Policy for the Information Society, Vol. 4, Issue 3, pp. 543-562.

McDonald, Aleecia M.; Cranor, Lorrie Faith (2008b): The cost of reading privacy policies; in: I/S: A Journal of Law and Policy for the Information Society, Vol. 4, Issue 3, pp. 543-568.

Miller, Akiva A. (2014): What Do We Worry About When We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing; in: Journal of Technology Law & Policy, Vol. 19, Issue 1, pp. 41-104.

Milne, George R.; Culnan, Mary J. (2004): Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices; in: Journal of Interactive Marketing, Vol. 18, Issue 3, pp. 15-29.

Mittelstadt, Brent Daniel; Allo, Patrick; Taddeo, Mariarosaria; Wachter, Sandra; Floridi, Luciano (2016): The ethics of algorithms: Mapping the debate; in: Big Data & Society, Vol. 3, Issue 2, pp. 1-21.

Moll, Ricarda; Horn, Marco; Scheibel, Lisa; Rusch-Rodosthenous, Miriam (2018): Soziale Medien und die EU-Datenschutzgrundverordnung. Informationspflichten und datenschutzfreundliche Voreinstellungen; Düsseldorf: Marktwächter Digitale Welt, Verbraucherzentrale NRW e.V.

Niemann, Antje; Schwaiger, Manfred (2016): Consumers' Expectations of Fair Data Collection and Usage - A Mixed Method Analysis, at: 2016 49th Hawaii International Conference on System Sciences (HICSS); published by IEEE.

Nissenbaum, Helen (2004): Privacy as Contextual Integrity; in: Washington Law Review, Vol. 79, Issue 1, pp. 119-157.

Nissenbaum, Helen (2010): Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford: Stanford University Press.

Nissenbaum, Helen (2011): A Contextual Approach to Privacy Online; in: Daedalus, Vol. 140, Issue 4, pp. 32-48.

Obar, Jonathan A.; Oeldorf-Hirsch, Anne (2016): The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services, at: TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy 2016.

OECD (2015): ISCED 2011 Operational Manual. Guidelines for Classifying National Education Programmes and Related Qualifications; Paris: Organisation for Economic Co-operation and Development (OECD).

Ohm, Paul (2010): Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization; in: UCLA Law Review, Vol. 57, Issue 6, pp. 1701-1777.

Penney, Jonathon W. (2016): Chilling Effects: Online Surveillance and Wikipedia Use; in: Berkeley Technology Law Journal, Vol. 31, Issue 1, pp. 117-182.

Penney, Jonathon W. (2017): Internet surveillance, regulation, and chilling effects online: a comparative case study; in: Internet Policy Review, Vol. 6, Issue 2.

Raabe, Oliver; Wagner, Manuela (2016a): Die Zweckbindung: Ein Überblick über die aktuelle Rechtslage und Harmonisierung durch die EU-Datenschutzgrundverordnung, in: Smart-Data-Begleitforschung (ed.): Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data. Datenschutzgrundprinzipien im Diskurs, Berlin: Smart-Data-Begleitforschung, pp. 16-22.

Raabe, Oliver; Wagner, Manuela (2016b): Verantwortlicher Einsatz von Big Data. Ein Zwischenfazit zur Entwicklung von Leitplanken für die digitale Gesellschaft; in: Datenschutz und Datensicherheit - DuD, Vol. 40, Issue 7, pp. 434-439.

Rainie, Lee; Duggan, Maeve (2016): Privacy and Information Sharing; Washington, D.C.: Pew Research Center.

Reidenberg, Joel R.; Bhatia, Jaspreet; Breaux, Travis D.; Norton, Thomas B. (2016): Ambiguity in privacy policies and the impact of regulation; in: The Journal of Legal Studies, Vol. 45, Issue S2, pp. S163-S190.

Reidenberg, Joel R.; Russell, N. Cameron; Callen, Alexander J.; Qasir, Sophia; Norton, Thomas B. (2015): Privacy harms and the effectiveness of the notice and choice framework; in: I/S: A Journal of Law and Policy for the Information Society, Vol. 11, Issue 2, pp. 485-524.

Root, Teri; McKay, Sandra (2014): Student Awareness of the Use of Social Media Screening by Prospective Employers; in: Journal of Education for Business, Vol. 89, Issue 4, pp. 202-206.

Rosenblat, Alex; Kneese, Tamara; boyd, danah (2014): Networked Employment Discrimination; Open Society Foundations' Future of Work Commissioned Research Papers 2014, New York: Data & Society Research Institute.

Roßnagel, Alexander; Geminn, Christian; Jandt, Silke; Richter, Philipp (2016): Datenschutzrecht 2016 - „Smart" genug für die Zukunft? Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts, Kassel: Kassel University Press.

Roßnagel, Alexander; Nebel, Maxi (2015): (Verlorene) Selbstbestimmung im Datenmeer; in: Datenschutz und Datensicherheit - DuD, Vol. 39, Issue 7, pp. 455-459.

Roßnagel, Alexander; Richter, Philipp (2016): Big data and Informational Self-Determination. Regulative Approaches in Germany: the Case of Police and Intelligence Agencies, in: van der Sloot, Bart; Broeders, Dennis; Schrijvers, Erik (eds.): Exploring the Boundaries of Big Data, Amsterdam: Amsterdam University Press, pp. 261-281.

Röttgen, Charlotte (2018): Like or Dislike - Web Tracking, in: Hoeren, Thomas; Kolany-Raiser, Barbara (eds.): Big Data in Context. Legal, Social and Technological Insights; Springer Briefs in Law, Cham: Springer Open, pp. 73-79.

Rouvroy, Antoinette (2016): "Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data; Strasbourg: Council of Europe; Directorate General of Human Rights and Rule of Law; Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

Rouvroy, Antoinette; Poullet, Yves (2009): The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy, in: Gutwirth, Serge; Poullet, Yves; De Hert, Paul; de Terwangne, Cécile; Nouwt, Sjaak (eds.): Reinventing Data Protection?, Amsterdam: Springer, pp. 45-76.

Rubinstein, Ira S. (2013): Big Data: The End of Privacy or a New Beginning?; in: International Data Privacy Law, Vol. 3, Issue 2, pp. 74-87.

Schneider, Ingrid; Ulbricht, Lena (2018): Ist Big Data fair? Normativ hergestellte Erwartungen an Big Data, in: Kolany-Raiser, Barbara; Heil, Reinhard; Orwat, Carsten; Hoeren, Thomas (eds.): Big Data und Gesellschaft. Eine multidisziplinäre Annäherung, Wiesbaden: Springer VS, pp. 198-207.

Schroeder, Amber N.; Cavanaugh, Jacqulyn M. (2018): Fake it 'til you make it: Examining faking ability on social media pages; in: Computers in Human Behavior, Vol. 84, Issue Jul., pp. 29-35.

Schwaiger, Manfred; Hufnagel, Gerrit (2018): Handel und elektronische Bezahlsysteme; Gutachten im Rahmen des Projekts "Assessing Big Data" (ABIDA), München: Ludwig-Maximilians-Universität München, Institut für Marktorientierte Unternehmensführung.

Schwartz, Paul M. (1999): Privacy and democracy in cyberspace; in: Vanderbilt Law Review, Vol. 52, Issue 6, pp. 1607-1702.

Schwartz, Shalom H. (2003a): Computing Scores for the 10 Human values; London: European Social Survey (ESS).

Schwartz, Shalom H. (2003b): A Proposal for Measuring Value Orientations across Nations. Chapter 7 in the Questionnaire Development Package of the European Social Survey; London: European Social Survey (ESS)

Schwartz, Shalom H.; Breyer, Bianka; Danner, Daniel (2015): Human Values Scale (ESS). Zusammenstellung sozialwissenschaftlicher Items und Skalen; Mannheim: GESIS - Leibniz-Institut für Sozialwissenschaften.

Simitis, Spiros (ed.) (2014): Bundesdatenschutzgesetz, 8., neu bearbeitete Auflage, Baden-Baden: Nomos.

Singer, Natasha (2012): You for sale - Mapping, and Sharing, the Consumer Genome, in: New York Times, June 16, 2012; available at: http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html (last access at: 2017-09-19).

Smith, H. Jeff; Dinev, Tamara; Xu, Heng (2011): Information privacy research: an interdisciplinary review; in: MIS Quarterly, Vol. 35, Issue 4, pp. 989-1016.

Solove, Daniel J. (2013): Privacy Self-Management and the Consent Dilemma; in: Harvard Law Review, Vol. 126, Issue 7, pp. 1880-1903.

Statistisches Bundesamt (2016): Private Haushalte in der Informationsgesellschaft – Nutzung von Informations- und Kommunikationstechnologien. Fachserie 15 Reihe 4; Wiesbaden: Statistisches Bundesamt.

Steinebach, Martin; Winter, Christian; Halvani, Oren; Schäfer, Marcel; Yannikos, York (2015): Chancen durch Big Data und die Frage des Privatsphärenschutzes. Begleitpapier Bürgerdialog. Big Data und Privatheit; Darmstadt: Fraunhofer Institut für Sichere Informationstechnologie (SIT).

Steppe, Richard (2017): Online price discrimination and personal data: A General Data Protection Regulation perspective; in: Computer Law & Security Review, Vol. 33, Issue 6, pp. 768-785.

Swedloff, Rick (2014): Risk classification's big data (r) evolution; in: Connecticut Insurance Law Journal, Vol. 21, Issue 1, pp. 339-373.

Taylor, G. Stephen; Davis, J. Stephen (1989): Individual privacy and computer-based human resource information systems; in: Journal of Business Ethics, Vol. 8, Issue 7, pp. 569-576.

ten Have, Marieke (2013): Lifestyle Differentiation in Health Insurance. An Overview of the Ethical Arguments; Monitoring Report on Ethics and Health 2013, The Hague: Netherlands Centre for Ethics and Health.

TFEU (2012): Consolidated version of the Treaty on the Functioning of the European Union; in: Official Journal of the European Union, Issue C 326, 26.10.2012, pp. 47-390.

The White House (2014): Big Data: Seizing Opportunities, Preserving Values; Washington, D.C.: The White House, Executive Office of the President.

The White House (2016): Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights; Washington, D.C.: The White House, Executive Office of the President.

Tillmann, Tristan Julian; Vogt, Verena (2018): Personalisierte Preise - Diskriminierung 2.0?; ABIDA-Dossier, Münster, Karlsruhe: Projekt "Assessing Big Data" (ABIDA).

Turow, Joseph; Feldman, Lauren; Meltzer, Kimberly (2005): Open to exploitation: America's shoppers online and offline; Departmental Papers, Annenberg Public Policy Center (ASC), Philadelphia: University of Pennsylvania, Annenberg Public Policy Center.

Turow, Joseph; King, Jennifer; Hoofnagle, Chris Jay; Bleakley, Amy; Hennessy, Michael (2009): Americans reject tailored advertising and three activities that enable it; Philadelphia, Berkeley: Annenberg School for Communication, University of Pennsylvania; Berkeley Center for Law & Technology, Berkeley, School of Law, University of California.

ULD; GP Forschungsgruppe (2014): Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen. Abschlussbericht; Kiel, München: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD); GP Forschungsgruppe.

Umhoefer, Carol; Rofé, Jonathan; Lemarchand, Stéphane; Baltassis, Elias; Stragier, François; Telle, Nicolas (2015): Earning Consumer Trust in Big Data: A European Perspective; DLA Piper and The Bosten Consulting Group (BCG).

US CEA (2015): Big Data and Differential Pricing; Washington D.C.: Council of Economic Advisers (CEA), Executive Office of the President of the United States.

US GAO (2013): Information Resellers - Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace (GAO-13-663); Washington, D.C.: United States Government Accountability Office (US GAO).

Van Alsenoy, Brendan; Kosta, Eleni; Dumortier, Jos (2014): Privacy notices versus informational self-determination: Minding the gap; in: International Review of Law, Computers and Technology, Vol. 28, Issue 2, pp. 185-203.

Van Slyke, Craig; Shim, J. T.; Johnson, Richard; Jiang, James J. (2006): Concern for information privacy and online consumer purchasing; in: Journal of the Association for Information Systems, Vol. 7, Issue 1, p. 16.

Varian, Hal R. (2010): Computer Mediated Transactions; in: The American Economic Review, Vol. 100, Issue 2, pp. 1-10.

Varian, Hal R. (2014): Beyond Big Data; in: Business Economics, Vol. 49, Issue 1, pp. 27-31.

Vicknair, Jamie; Elkersh, Dalia; Yancey, Katie; Budden, Michael C. (2010): The use of social networking websites as a recruiting tool for employers; in: American Journal of Business Education, Vol. 3, Issue 11, p. 7.

Vodafone Institut (2016): Big Data - Wann Menschen bereit sind, ihre Daten zu teilen. Eine Europäische Studie; Berlin: Vodafone Institut für Gesellschaft und Kommunikation GmbH.

Wachter, Sandra; Mittelstadt, Brent; Floridi, Luciano (2017): Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation; in: International Data Privacy Law, Vol. 7, Issue 2, pp. 76-99.

Wei, Yanhao; Yildirim, Pinar; Van den Bulte, Christophe; Dellarocas, Chrysanthos (2016): Credit Scoring with Social Network Data; in: Marketing Science, Vol. 35, Issue 2, pp. 234-258.

Weichert, Thilo (2013): Big Data und Datenschutz - Chancen und Risiken einer neuen Form der Datenanalyse; in: Zeitschrift für Datenschutz, Vol. 3, Issue 6, pp. 251-259.

Weichert, Thilo (2014): Scoring in Zeiten von Big Data; in: Zeitschrift für Rechtspolitik (ZRP), Vol. 47, Issue 6, pp. 168-171.

Weichert, Thilo (2018): Big Data im Gesundheitsbereich; Gutachten im Rahmen des Projekts "Assessing Big Data" (ABIDA), Münster, Karlsruhe: Universität Münster; Karlsruher Institut für Technologie.

Wright, David; Watson, Hayley; Finn, Rachel L.; Székely, Iván; Raab, Charles D.; Goos, Kerstin; Friedewald, Michael (2013): Report on Existing Surveys. Deliverable 7.1; Report by the Project PRISMS - The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making.

Yeung, Karen (2016): 'Hypernudge': Big Data as a mode of regulation by design; in: Information, Communication & Society, Vol. 20, Issue 1, pp. 1-19.

Zander-Hayat, Helga; Reisch, Lucia A.; Steffen, Christine (2016): Personalisierte Preise: Eine verbraucherpolitische Einordnung; in: Verbraucher und Recht, Vol. 31, Issue 11, pp. 403-409.

Zarsky, Tal Z. (2014): Understanding discrimination in the scored society; in: Washington Law Review, Vol. 89, Issue 4, pp. 1375-1412.

Zarsky, Tal Z. (2016): The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making; in: Science, Technology & Human Values, Vol. 41, Issue 1, pp. 118-132.

Zuboff, Shoshana (2015): Big other: surveillance capitalism and the prospects of an information civilization; in: Journal of Information Technology, Vol. 30, Issue 1, pp. 75-89.

Zuiderveen Borgesius, Frederik; Poort, Joost (2017): Online Price Discrimination and EU Data Privacy Law; in: Journal of Consumer Policy, Vol. 40, Issue 3, pp. 347-366.

Appendix A Tables with detailed results

Table A.1: Self-assessment of knowledge about computers and internet use

	Percent (%) of population				
Description of items	**1 = No knowledge**	**2**	**3**	**4**	**5 = Comprehensive knowledge**
Knowledge of using PCs in general, including laptops	2.6	12.9	30.7	26.4	14.5
Knowledge of using the internet with PCs	3.4	9.3	30.4	26.2	17.8
Knowledge of using the internet with smartphones	14.5	11.0	25.0	20.5	16.1
Knowledge of using apps on tablets and smartphones	16.4	14.3	22.9	22.0	11.5
Knowledge of using devices connected to the internet, e.g. connected TVs or stereo systems	30.5	14.1	20.6	13.3	8.1

Notes: N = 1,331. 170 respondents with no computer and internet use or with no answers are not shown here. Order of items follows that of Figure 7.1.

Table A.2: Attitudes towards privacy and data protection

	Percent (%) of population				
Description of items	**1 = Do not agree at all**	**2**	**3**	**4**	**5 = Fully agree**
I am worried about the fact that companies collect and transfer more and more data about me, without my knowing.	9.1	6.5	9.4	13.9	48.3
I often think about what data about me are produced and what happens to them.	10.6	9.8	20.4	14.4	31.9
I have no time to think about the topic of data protection.	32.8	14.0	21.9	8.2	10.0
I agree to data about being collected and processed, if I can use the respective services free of charge.	32.6	15.5	19.9	10.4	7.8
I gave up thinking about the use of data.	37.4	13.4	17.7	7.4	11.1
I don't really care what happens to data about me.	60.1	11.0	7.5	2.6	6.0

Notes: N = 1,331. 170 respondents with no computer and internet use or with no answers are not shown here. Order of items follows that of Figure 7.2. Numerical values of responses (1 to 5) were re-orientated in order to get directions in answering similar to other figures, verbal answering options (Do not agree at all, fully agree) remain the same. Items read in random order to respondents.

Table A.3: Assessment of scenario statements

	Percent (%) of population					
Description of items (item number)	**5**[a]	**4**	**3**	**2**	**1**[a]	**Not specified**
Differentiation						
(S3) I think this would be difficult to understand.	3.61	6.54	13.82	22.69	53.04	0.30
(S5) I believe that the [company] would only try to increase its profit.	3.76	7.74	16.30	23.74	48.38	0.08
(S6) I would feel disadvantaged, because I might finally [have to pay] more than before.	9.84	14.43	22.46	22.92	29.60	0.75
(S4) I believe that the comparability and competition on the markets would suffer from this.	6.69	15.78	28.25	26.90	21.56	0.83
(S2) I think that [conditions] adapted in this way are a good thing, because they better match the needs of the respective person.	25.02	23.67	21.41	17.73	11.80	0.38
(S1) I think that is a good idea if one can benefit from it [...].	30.73	23.14	20.59	15.10	10.29	0.15
Use of internet data						
(S8) I think this would be too much of an intrusion into privacy and should be prohibited.	1.95	3.01	7.51	13.15	73.10	1.28
(S9) I believe that this would be too prone to errors and one could hardly take action against such errors.	2.18	3.76	11.80	23.82	56.65	1.80
(S7) I think, in this way, the [company] could better understand [me in specific roles, my characteristics].	31.71	14.88	22.31	13.82	15.85	1.43
(S10)* All in all, how do you feel about the situation when decisions are made based on large amounts of data?	61.38	25.39	8.41	3.53	0.98	0.30
Automated decision-making						
(S14) I think it should be prohibited that computers make such decisions on their own. A human must always control.	1.35	2.63	8.11	11.50	75.96	0.45
(S13) I think in this case the computer should only give recommendations and the human should always decide.	1.35	3.98	8.11	15.63	70.02	0.90
(S11) I believe in this case the computer could make better decisions than a human.	58.53	21.19	10.37	5.56	2.85	1.50
(S12) I think it's right that a computer makes such decisions alone and without human control.	79.79	11.72	4.28	2.48	0.45	1.28
(S15)* How do you feel about computers making such decisions without human control?	83.32	12.17	2.40	1.95	0.15	0.00
Behavioural adaptations						
(S19) I would take measures to better protect my privacy, e.g. [...].	1.13	1.80	5.71	12.17	57.55	21.64
(S17) I would be careful not to reveal anything negative about me on the internet.	2.93	0.98	4.66	8.26	61.68	21.49
(S18) I would, for instance, make entries in social networks or other websites which put me intentionally in a favourable light.	14.50	8.26	16.60	12.85	22.24	25.54
(S16) I would not change my behaviour and my communication on the internet.	32.61	17.21	16.30	13.22	15.40	5.26
Protection measures						
(S20) I think I should have easy control options over what data about me is collected and how it is used.	2.33	2.18	8.11	13.00	73.93	0.45
(S23) I wish that the state would regulate and enforce what data may be used.	4.06	4.96	11.12	18.56	60.63	0.68
(S22) It would be fine with me if the [company] transferred the data in anonymised form to third parties for purposes of [research].	36.44	22.09	16.98	13.75	10.67	0.08
(S21) From my point of view, the [company] can sell the data to other companies.	89.41	5.86	2.85	1.13	0.60	0.15

Notes: N = 1,331. Table presents the percent of the frequency of the means of the four scenarios. Means were regrouped before analysis in order to achieve comparability with other results of the study. Numerical values are rounded to two decimal places. Item numbers and order of items are from Figure 7.3. Items were read in random order to respondents within sections 'Differentiation', 'Use of internet data', 'Automated decision-making', 'Behavioural adaptations', and 'Protection measures'. [a]Answering options were anchored with 5 = Do not agree at all and 1 = Fully agree. Items marked with an asterisk (*) had answering options anchored with 5 = feel very uncomfortable and 1 = feel very comfortable.

Table A.4: Attitudes towards big data practices and potential moderators

Description of item		Gender	Age group	Education	Income	Frequency of use	Computer knowledge	Privacy self-management
	df	4	28	12	16	20	8	4
(S1) I think that is a good idea if one can benefit from it [...].	χ^2	14.125**[a]	70.455***[a]	74.731***	26.101	65.638***	31.743***	15.679**
	V	**0.103**	**0.115**	**0.137**	0.077	**0.111**	**0.117**	**0.116**
(S2) I think that [conditions] adapted in this way are a good thing, because they better match the needs of the respective person.	χ^2	12.137*[a]	64.320***[a]	54.755***	50.822***	69.852***	17.133	19.205***
	V	0.096	**0.110**	**0.117**	**0.107**	**0.115**	0.086	**0.129**
(S4) I believe that the comparability and competition on the markets would suffer from this.	χ^2	11.837*[a]	91.674***[a]	27.927**	53.337***	54.366***	7.313	18.333**
	V	0.095	**0.132**	0.084	**0.110**	**0.102**	0.056	**0.126**
(S6) I would feel disadvantaged, because I might finally [have to pay] more than before.	χ^2	7.910[a]	127.633***[a]	60.779***	29.340*	48.039***	29.043***	8.316
	V	0.077	**0.155**	**0.124**	0.081	0.095	**0.112**	0.085
(S7) I think, in this way, the [company] could better understand [me in specific roles, my characteristics].	χ^2	8.306[a]	70.817***[a]	51.428***	55.224***	44.138**	5.835	6.882
	V	0.080	**0.116**	**0.115**	**0.112**	0.092	0.050	0.077
(S16) I would not change my behaviour and my communication on the internet.	χ^2	9.910*	72.292***[a]	25.356*	20.316	37.389*	33.774***	15.323**
	V	0.089	**0.120**	0.082	0.070	0.086	**0.121**	**0.116**
(S18) I would, for instance, make entries in social networks or other websites which put me intentionally in a favourable light.	χ^2	12.286*[a]	90.872***[a]	32.875**	36.896**	60.682***	38.557***	17.765**
	V	**0.111**	**0.151**	**0.105**	**0.106**	**0.124**	**0.147**	**0.141**
(S22) It would be fine with me if the [company] transferred the data in anonymised form to third parties for purposes of [research].	χ^2	0.904	58.823***[a]	72.974***	29.794*	42.611**	17.982*	9.951*
	V	0.026	**0.105**	**0.136**	0.082	0.090	0.088	0.093

Notes: *p < 0.050, **p < 0.010, ***p < 0.001. Table depicts chi-square (χ2) values, Cramérs' V (V), degree of freedom (df), and significance (p). Weak effect sizes (V < 0.3) in bold. Values calculated with exact tests. [a]Significance calculated with exact test. [b]More than 20 percent expected cell counts smaller than 5. Item numbers are from Figure 7.3.

Table A.5: Attitudes towards big data practices and personal value orientations

		Personal value orientations									
Description of item		**Self-direction**	**Power**	**Universalism**	**Achievement**	**Security**	**Stimulation**	**Conformity**	**Tradition**	**Hedonism**	**Benevolence**
(S1) I think that is a good idea if one can benefit from it [...].	F(4, 1248)	9.737***	4.798***	9.225***	11.735***	2.968*	2.693*	2.731*	2.218	1.958	7.853***
	η_p^2	**0.030**	**0.015**	**0.029**	**0.036**	0.009	0.009	0.009	0.007	0.006	**0.025**
(S2) I think that [conditions] adapted in this way are a good thing, because they better match the needs of the respective person.	F(4, 1247)	4.489**	9.021***	7.990***	11.282***	4.964***	3.464**	3.453**	2.121	1.282	2.937*
	η_p^2	**0.014**	**0.028**	**0.025**	**0.035**	**0.016**	**0.011**	**0.011**	0.007	0.004	0.009
(S4) I believe that the comparability and competition on the markets would suffer from this.	F(4, 1239)	3.515**	4.026**	2.079	3.598**	3.023*	3.498**	7.668***	1.589	2.113	0.778
	η_p^2	**0.011**	**0.013**	0.007	**0.011**	0.010	**0.011**	**0.024**	0.005	0.007	0.003
(S6) I would feel disadvantaged, because I might finally [have to pay] more than before.	F(4, 1243)	2.169	5.959***	7.058***	9.689***	2.444*	4.586**	0.272	6.017***	1.718	5.469***
	η_p^2	0.007	**0.019**	**0.022**	**0.030**	0.008	**0.015**	0.001	**0.019**	0.005	**0.017**
(S7) I think, in this way, the [company] could better understand [me in specific roles, my characteristics].	F(4, 1233)	3.454**	1.364	2.054	3.903**	1.877	6.538***	2.846*	6.631***	3.430**	2.368
	η_p^2	**0.011**	0.004	0.007	**0.013**	0.006	**0.021**	0.009	**0.021**	**0.011**	0.008
(S16) I would not change my behaviour and my communication on the internet.	F(4, 1184)	1.894	7.219***	4.317**	3.495**	1.883	6.163***	2.928*	3.964**	0.260	2.779*
	η_p^2	0.006	**0.024**	**0.014**	**0.012**	0.006	**0.020**	0.010	**0.013**	0.001	0.009
(S18) I would, for instance, make entries in social networks or other websites which put me intentionally in a favourable light.	F(4, 928)	1.880	9.976***	5.360***	6.021***	8.161***	3.439**	4.719***	6.311***	1.686	0.699
	η_p^2	0.008	**0.041**	**0.023**	**0.025**	**0.034**	**0.015**	**0.020**	**0.026**	0.007	0.003
(S22) It would be fine with me if the [company] transferred the data in anonymised form to third parties for purposes of [research].	F(4, 1247)	1.103	2.160	2.641*	2.094	2.603*	1.317	2.975*	0.485	0.703	1.882
	η_p^2	0.004	0.007	0.008	0.007	0.008	0.004	0.009	0.002	0.002	0.006

Notes: *p < 0.050, **p < 0.010, ***p < 0.001. Weak effect sizes ($0.01 < \eta_p^2 < 0.06$) in bold. Item numbers are from Figure 7.3.

Table A.6: Reading and understanding of privacy policies and potential moderators

		Gender	Age group	Education	Income	Frequency of computer use	Knowledge about computers and internet	Privacy self-management	Term big data known	Associations with term big data
How often do you read the privacy policies at least partly?	χ^2	20.715***[a]	106.360***[a]	75.212***	18.610	127.245***	6.390	25.000***	8.854	13.656
	df	4	28	12	16	20	8	4	4	12
	V	**0.127**	**0.143**	**0.140**	0.066	**0.157**	0.053	**0.147**	0.083	0.097
If you have read the privacy policies how often do you feel that you have largely understood them?	χ^2	2.905	64.426***[a]	49.358***	31.734*	69.451***	75.894***	17.753**	31.220***	11.775
	df	4	28	12	16	20	8	4	4	12
	V	0.053	**0.125**	**0.126**	0.096	**0.129**	**0.198**	**0.136**	**0.174**	0.100

Notes: $^*p < 0.050$, $^{**}p < 0.010$, $^{***}p < 0.001$. Table depicts chi-square ($\chi2$) values, Cramérs' V (V), degree of freedom (df), and significance (p). Weak effect sizes (V < 0.3) in bold. [a]Significance calculated with exact test. All expected cell counts smaller than 5.

Table A.7: Reading and understanding of privacy policies and personal value orientations

		Personal value orientations									
Description of item		**Self-direction**	**Power**	**Universalism**	**Achievement**	**Security**	**Stimulation**	**Conformity**	**Tradition**	**Hedonism**	**Benevolence**
How often do you read the privacy policies at least partly?	F(4, 1210)	3.458**	2.291	3.227*	3.553**	0.849	6.663***	1.037	0.242	1.433	6.527***
	η_p^2	**0.011**	0.008	**0.011**	**0.012**	0.003	**0.022**	0.003	0.001	0.005	**0.021**
If you have read the privacy policies how often do you feel that you have largely understood them?	F(4, 973)	1.928	2.450*	5.226***	2.776*	0.743	0.445	1.313	4.387**	1.441	1.414
	η_p^2	0.008	0.010	**0.021**	**0.011**	0.003	0.002	0.005	**0.018**	0.006	0.006

Notes: $^*p < 0.050$, $^{**}p < 0.010$, $^{***}p < 0.001$. Weak effect sizes ($0.01 < \eta_p^2 < 0.06$) in bold.

Table A.8: Attitudes towards purpose limitation

	Percent (%) of population				
Description of items	**1 = Do not agree at all**	**2**	**3**	**4**	**5 = Fully agree**
I believe that companies are not honest when it comes to using of data about me.	5.4	6.2	19.4	18.0	48.5
I believe that new data about me is generated without my knowing or haven consented to it.	8.8	6.9	13.4	15.9	51.0
I believe that companies adhere to the data processing purposes described in their policies and do nothing else with the data.	37.6	18.7	25.2	6.8	8.3
I think companies always ask me when data is used for other purposes.	47.3	15.9	15.2	10.0	8.4
I think companies always ask me when data is transferred to third parties.	49.7	17.5	12.8	7.2	10.0
I think companies clearly and comprehensively inform me of what data about me are being processed.	47.3	21.1	14.1	5.4	8.2

Notes: N = 1,331. Respondents whose answers cannot be specified are not shown here. Items were read in random order to respondents. Numerical values of responses (1 to 5) were re-orientated in order to get directions in answering similar to other figures. Verbal answering options (Do not agree at all, fully agree) remain the same. Order of items follows that of Figure 7.5.

Table A.9: Attitudes towards purpose limitation and potential moderators

		Gender	**Age group**	**Education**	**Income**	**Frequency of computer use**	**Knowledge about computers and internet**	**Privacy self-management**	**Term big data known**	**Associations with term big data**
I believe that companies adhere to the data processing purposes described in their policies and do nothing else with the data.	χ^2	7.807	52.820***[a]	57.060***	21.914	74.373***	31.543***	4.940	5.796	24.177*
	df	4	28	12	16	20	8	4	4	12
	V	0.078	**0.101**	**0.122**	0.071	**0.121**	**0.118**	0.066	0.067	**0.129**
I think companies clearly and comprehensively inform me of what data about me are being processed.	χ^2	5.007	117.879***[a]	54.640***	12.221	89.147***	21.484**	11.412*	30.091***	34.786***
	df	4	28	12	16	20	8	4	4	12
	V	0.063	**0.152**	**0.120**	0.053	**0.132**	0.097	**0.100**	**0.153**	**0.155**
I think companies always ask me when data are used for other purposes.	χ^2	9.584*[a]	92.543***[a]	86.525***	39.358***	53.311***	18.096*	7.142	14.685**	21.795*
	df	4	28	12	16	20	8	4	4	12
	V	0.086	**0.134**	**0.150**	0.095	**0.102**	0.089	0.079	**0.107**	**0.123**
I think companies always ask me when data are transferred to third parties.	χ^2	2.851	76.208***[a]	72.076***	14.923	38.958**	15.616*	3.141	24.245***	22.053*
	df	4	28	12	16	20	8	4	4	12
	V	0.047	**0.121**	**0.136**	0.059	0.087	0.082	0.052	**0.137**	**0.123**
I believe that companies are not honest when it comes to using data about me.	χ^2	4.737	114.554***[a]	97.037***	39.663***	80.075***	53.648***	8.619	16.662**	17.853
	df	4	28	12	16	20	8	4	4	12
	V	0.060	**0.148**	**0.158**	0.096	**0.124**	**0.153**	0.087	**0.113**	**0.111**
I believe that new data about me are generated without my knowing or having consented to it.	χ^2	15.234**	102.795***[a]	50.614***	68.488***	62.007***	18.592	8.608	26.707***	23.009
	df	4	28	12	16	20	8	4	4	12
	V	**0.109**	**0.142**	**0.115**	**0.126**	**0.110**	0.091	0.087	**0.145**	**0.126**[b]

Notes: *p < 0.050, **p < 0.010, ***p < 0.001. Table depicts chi-square (χ2) values, Cramérs' V (V), degree of freedom (df), and significance (p). Weak effect sizes (V < 0.3) in bold. [a]Significance calculated with exact test. [b]More than 20 percent expected cell counts smaller than 5.

Table A.10: Attitudes towards purpose limitation and personal value orientations

		Personal value orientations									
		Self-direction	**Power**	**Universalism**	**Achievement**	**Security**	**Stimulation**	**Conformity**	**Tradition**	**Hedonism**	**Benevolence**
I believe that companies adhere to the data processing purposes described in their policies and do nothing else with the data.	F(4,1213)	1.322	5.681***	2.840*	3.154*	4.158**	1.711	2.367	2.012	0.090	7.049***
	η_p^2	0.004	**0.018**	0.009	**0.010**	**0.014**	0.006	0.008	0.007	0.000	**0.023**
I think companies clearly and comprehensively inform me of what data about me are being processed.	F(4,1212)	3.462**	1.989	3.707**	9.202***	2.094	5.762***	3.266*	5.890***	1.403	8.534***
	η_p^2	**0.011**	0.007	**0.012**	**0.029**	0.007	**0.019**	**0.011**	**0.019**	0.005	**0.027**
I think companies always ask me when data are used for other purposes.	F(4,1209)	1.631	2.619*	3.277*	5.955***	1.278	7.785***	1.952	6.786***	1.234	11.363***
	η_p^2	0.005	0.009	**0.011**	**0.019**	0.004	**0.025**	0.006	**0.022**	0.004	**0.036**
I think companies always ask me when data are transferred to third parties.	F(4, 1217)	6.033***	1.825	5.675***	8.937***	2.113	2.010	1.795	2.011	0.966	5.522***
	η_p^2	**0.019**	0.006	**0.018**	**0.029**	0.007	0.007	0.006	0.007	0.003	**0.018**
I believe that companies are not honest when it comes to using data about me.	F(4, 1216)	4.134**	9.852***	3.768**	5.576***	4.150**	2.766*	2.893*	4.695***	1.089	4.132**
	η_p^2	**0.013**	**0.031**	**0.012**	**0.018**	**0.013**	0.009	0.009	**0.015**	0.004	**0.013**
I believe that new data about me are generated without my knowing or having consented to it.	F(4, 1203)	8.102***	2.754*	2.318	4.770***	1.126	5.549***	3.916**	4.158**	1.321	5.003***
	η_p^2	**0.026**	0.009	0.008	**0.016**	0.004	**0.018**	**0.013**	**0.014**	0.004	**0.016**

Notes: *p < 0.050, **p < 0.010, ***p < 0.001. Weak effect sizes ($0.01 < \eta_p^2 < 0.06$) in bold.

Table A.11: Attitudes towards individuals' rights and potential moderators

		Gender	Age group	Education	Income	Frequency of computer use	Knowledge about computers and internet	Privacy self-management	Term big data known	Associations with term big data
Have you ever heard that you have a right to ask a company or an authority for information about the data they process about you?	χ^2	12.242**a	34.884***	33.193***	37.351***	52.647***	22.699***	9.397**	114.341***	2.714
	df	1	7	3	4	5	2	1	1	3
	V	0.096	**0.162**	**0.159**	**0.183**	**0.200**	**0.140**	0.090	**0.294**	0.075
Have you ever used this option and asked a company or an authority for information about what data they process about you?	χ^2	1.859	11.067	6.170	7.214	8.536	8.228*	4.966*	9.120**	1.903
	df	1	7	3	4	5	2	1	1	3
	V	0.054	**0.131**	0.098	**0.118**	**0.115**	**0.118**	0.092	**0.119**	0.077
Have you ever heard that you have a right to request correction of incorrect data or erasure of certain data about you?	χ^2	10.517**a	11.381	11.746**	15.959**	10.842	22.529***	2.208	27.479***	5.913
	df	1	7	3	4	5	2	1	1	3
	V	**0.127**	**0.133**	**0.135**	**0.175**	**0.130**	**0.195**	0.061	**0.206**	**0.135**
Have you ever used this option and requested correction or erasure of data about you?	χ^2	0.145	28.004***	3.134	1.913	13.006*	15.192***	5.795*	12.032***	1.852
	df	1	7	3	4	5	2	1	1	3
	V	0.016	**0.228**	0.076[b]	0.066	**0.156**[b]	**0.175**	**0.109**	**0.150**	0.080

Notes: *p < 0.050, **p < 0.010, ***p < 0.001. Table depicts chi-square (χ2) values, Cramérs' V (V), degree of freedom (df), and significance (p). Weak effect sizes (V < 0.3) in bold. [a]Significance calculated with exact test. [b]More than 20 percent expected cell counts smaller than 5.

Table A.12: Attitudes towards individuals' rights and personal value orientations

		Personal value orientations									
		Self-direction	Power	Universalism	Achievement	Security	Stimulation	Conformity	Tradition	Hedonism	Benevolence
Have you ever heard that you have a right to ask a company or an authority for information about the data they process about you?	F(1, 1248)	32.357***	8.278**	3.438	0.377	13.070***	10.577**	16.591***	15.749***	1.839	0.428
	η^2	**0.025**	0.007	0.003	0.000	**0.010**	0.008	**0.013**	**0.012**	0.001	0.000
Have you ever used this option and asked a company or an authority for information about what data they process about you?	F(1,599)	6.301*	1.075	1.057	5.595*	1.084	4.205*	9.654**	3.342	6.397*	0.402
	η^2	**0.010**	0.002	0.002	0.009	0.002	0.007	**0.016**	0.006	**0.011**	0.001
Have you ever heard that you have a right to request correction of incorrect data or erasure of certain data about you?	F(1, 599)	3.709	1.118	0.900	0.868	8.287**	1.310	1.693	1.821	3.449	0.223
	η^2	0.006	0.002	0.002	0.001	**0.014**	0.002	0.003	0.003	0.006	0.000
Have you ever used this option and requested correction or erasure of data about you?	F(1, 498)	6.910**	0.432	2.464	0.033	0.011	5.794*	23.753***	9.724**	9.714**	3.406
	η^2	**0.014**	0.001	0.005	0.000	0.000	**0.012**	**0.046**	**0.019**	**0.019**	0.007

Notes: *p < 0.050, **p < 0.010, ***p < 0.001. Weak effect sizes (0.01 < η_p^2 < 0.06) in bold.

Table A.13: Demands on data protection and potential moderators

		Gender	Age group	Education	Income	Frequency of computer use	Knowledge about computers and internet	Privacy self-management	Term big data known	Associations with term big data
Everyone is solely responsible for protecting their data.	χ^2	2.187	65.578***	73.692***	48.373***	46.580***	16.577**	3.039	44.262***	28.985***
	df	2	14	6	8	10	4	2	2	6
	V	0.041	**0.158**[b]	**0.167**	**0.148**	**0.133**[b]	0.085	0.051	**0.183**	**0.173**[b]
I know whom to contact in order to enforce my data protection rights.	χ^2	4.078	37.712**	18.311**	20.762**	12.929	37.100***	13.548**	9.683**	10.995
	df	2	14	6	8	10	4	2	2	6
	V	0.055	**0.119**[b]	0.083[b]	0.097[b]	0.070[b]	**0.127**[b]	**0.108**	0.085	**0.107**[b]
I would like to learn much more about computers, the internet, and data protection.	χ^2	1.306	86.102***	15.275*	15.180	94.114***	24.610***	11.894**	1.907	16.034*
	df	2	14	6	8	10	4	2	2	6
	V	0.032	**0.181**[b]	0.076	0.083[b]	**0.189**[b]	**0.103**	**0.102**	0.038	**0.129**[b]

Notes: *p < 0.050, **p < 0.010, ***p < 0.001. Table depicts chi-square (χ2) values, Cramérs' V (V), degree of freedom (df), and significance (p). Weak effect sizes (V < 0.3) in bold. [a]Significance calculated with exact test. [b]More than 20 percent expected cell counts smaller than 5.

Table A.14: Demands on data protection and personal value orientations

		Personal value orientations									
		Self-direction	Power	Universalism	Achievement	Security	Stimulation	Conformity	Tradition	Hedonism	Benevolence
Everyone is solely responsible for protecting their data.	F(2, 1242)	4.467*	6.724**	4.287*	1.543	8.154***	0.566	2.917	11.138***	1.715	2.694
	η^2	0.007	**0.011**	0.007	0.002	**0.013**	0.001	0.005	**0.018**	0.003	0.004
I know whom to contact in order to enforce my data protection rights.	F(2, 1247)	5.794**	1.656	0.134	0.008	1.331	3.081*	0.641	0.141	0.905	7.252***
	η^2	0.009	0.003	0.000	0.000	0.002	0.005	0.001	0.000	0.001	**0.011**
I would like to learn much more about computers, the internet, and data protection.	F(2, 1236)	4.983**	2.894	0.037	13.439***	0.203	5.265**	8.239***	0.723	1.764	2.026
	η^2	0.008	0.005	0.000	**0.021**	0.000	0.008	**0.013**	0.001	0.003	0.003

Notes: *p < 0.050, **p < 0.010, ***p < 0.001. Weak effect sizes ($0.01 < \eta_p^2 < 0.06$) in bold.

Appendix B Questionnaire

		German original	English translation
Demographics			
Gender	q1	Sind Sie männlich oder weiblich?	Are you male or female?
Age	q2	Wie alt sind Sie?	How old are you?
Household size	q3a	Wie viele Personen leben ständig in Ihrem Haushalt, Sie selbst mit eingeschlossen?	How many persons live permanently in your household, including yourself?
	q3b	Wie viele Personen davon sind unter 18 Jahre alt?	How many of them are under the age of 18?
Questions on use of and knowledge about computers and internet, and about privacy and data protection			
Frequency of computer and internet use	q4	Wie oft nutzen Sie Computer und das Internet? Denken Sie bitte an die letzten vier Wochen, sowohl an Ihre Arbeit als auch an Ihre Freizeit und an die Nutzung mit verschiedenen Geräten, d.h. PCs als Desktop-Computer oder Laptops, Smartphones, Tablets oder mit dem Internet verbundene Geräte, wie vernetzte Fernseher bzw. Smart-TV. Nutzen Sie Computer und Internet ...	How often do you use computers and the internet? Please recall the last four weeks, both at work and in your free time, and the use of different devices, i.e. PCs as desktops or laptops, smartphones, tablets or other devices connected to the internet such as connected TVs or smart TVs respectively. Do you use computers and the internet ...
		praktisch den ganzen Tag	practically the whole day
		mehrmals täglich	several times in the day
		mehrmals in der Woche	several times in a week
		einmal pro Woche	once in a week
		seltener	less frequent
		nie	never
Self-assessment of knowledge about computers and the internet		Wie würden Sie Ihre Kenntnisse zu Computern und Internet selbst einschätzen? Bitte geben Sie dies jeweils auf einer Skala an von "1 = keine Kenntnisse" bis "5 = umfangreiche Kenntnisse": [Items in zufälliger Reihenfolge]	How would you assess your knowledge of computers and the internet? Please indicate on a scale from "1 = no knowledge" to "5 = comprehensive knowledge". [Items in random order]
	q51	Bei der Nutzung von PCs einschließlich Laptops im Allgemeinen	... of using PCs in general, including laptops
	q52	Bei der Internetnutzung mit PCs	... of using the internet with PCs
	q53	Bei der Internetnutzung mit Smartphones	... of using the internet with smartphones
	q54	Beim Umgang mit Apps auf Tablets oder Smartphones	... of using apps on tablets and smartphones
	q55	Bei Geräten, die mit dem Internet verbunden sind, z.B. vernetzte Fernseher oder Stereoanlagen	... of using devices connected to the internet, e.g. connected TVs or stereo systems
Attitudes towards data protection, in general		Ob bei der Internetnutzung, bei der Nutzung von Smartphones oder von Geräten, die mit dem Internet verbunden sind, es fallen immer mehr Daten über Personen und ihr Verhalten an. Wie sehr stimmen Sie den folgenden Aussagen zu, von „1 = stimme voll und ganz zu" bis „5 = stimme überhaupt nicht zu"? [Items in zufälliger Reihenfolge]	Whether it is the use of the internet or the use of smartphones or devices connected to the internet, more and more data about persons and their behaviour is collected. How much do you agree with the following statements, from "1 = fully agree" to "5 = do not agree at all". [Items in random order]
	q61	Ich bin bereit, dass Daten über mich erfasst und verarbeitet werden, wenn ich dafür die entsprechenden Dienste kostenlos nutzen kann.	I agree to data about me being collected and processed, if I can use the respective services free of charge.
	q62	Mir ist es eigentlich egal, was mit Daten über mich passiert.	I don't really care what happens to data about me.

	q63	Ich habe es aufgegeben, mir Gedanken über die Datenverwendung zu machen.	I gave up thinking about the use of data.
	q64	Ich habe keine Zeit über das Thema Datenschutz nachzudenken.	I have no time to think about the topic of data protection.
	q65	Ich mache mir Sorgen, dass Unternehmen immer mehr Daten über mich sammeln und weitergeben, ohne dass ich davon etwas weiß.	I am worried about the fact that companies collect and transfer more and more data about me, without my knowing.
	q66	Ich mache mir oft Gedanken, welche Daten von mir erzeugt werden und was mit ihnen passiert.	I often think about what data about me are produced and what happens to them.
Privacy self-management		Welche der folgenden Maßnahmen zum Datenschutz haben Sie in den letzten zwölf Monaten getroffen? Bitte antworten Sie hier jeweils mit „ja" oder „nein": [Items in zufälliger Reihenfolge, bis auf letztes]	Which of the following measures of data protection have you taken within the last 12 month? Please answer with "yes" or "no": [Items in random order, except last one]
	q71	Ich nutze E-Mail-Programme bzw. E-Mail-Anbieter, die für mehr Datenschutz bekannt sind.	I use e-mail programs or e-mail providers that are known for better data protection.
	q72	Wenn ich mich bei Internetdiensten anmelde, verwende ich oft nicht meinen richtigen Namen.	When registering for internet services, I often do not use my real name.
	q73	Ich habe bei meinem Browser, also dem Programm zum Surfen im Internet, Einstellungen für mehr Datenschutz vorgenommen, z.B. das Akzeptieren von Cookies untersagt.	I have changed the settings of my browser, i.e. the program for surfing the internet, for better data protection, e.g. by preventing cookies from being set.
	q74	Wenn dies möglich ist, installiere ich auf meinem Smartphone oder Tablet auch Apps, die als datenschutzfreundlicher gelten.	If possible, I install apps on my smartphone or tablet that are considered more privacy-enhancing.
	q75	Ich nutze regelmäßig Suchmaschinen im Internet, die als verhältnismäßig datenschutzfreundlich gelten, z.B. DuckDuckGo, Startpage, Ixquick.	I regularly use search engines on the internet that are considered relatively privacy-friendly, e.g. DuckDuckgo, Startpage or Ixquick.
	q76	Ich ergreife beim Surfen im Internet oft Maßnahmen, um meine Datenspuren zu verschleiern, z.B. VPN-Verbindungen oder den Tor-Browser.	When surfing the internet, I often take measures to obscure my data traces, e.g. VPN connections or the Tor browser.
	q77	Ich habe bestimmten Internetdiensten oder Apps den Zugriff auf meinen Standort untersagt.	I have denied access to my location for certain internet services or apps.

Scenarios on big data practices

Scenario 'Retail': Differentiation		Stellen Sie sich vor, Sie sind in einem Geschäft und es werden speziell für Sie festgelegte Preise berechnet. Die Preise werden auf der Grundlage eines Kundenprofils berechnet, welches das Geschäft von Ihnen angelegt hat. Bitte geben Sie auf einer Skala von „1 = stimme voll und ganz zu" bis „5 = stimme überhaupt nicht zu" an, wie stark Sie den folgenden Aussagen zustimmen: [Items in zufälliger Reihenfolge]	Imagine you are in a shop and you are charged prices especially calculated and set for you. The prices are calculated on the base of your customer profile created by the shop. Please indicate on a scale from "1 = fully agree" to "5 = do not agree at all" how much you do agree with the following statements: [Items in random order]
(for scenario item S1)	q81	Ich finde das eine gute Idee, wenn man dadurch Vorteile erhalten kann, wie z.B. regelmäßige Rabatte.	I think that is a good idea if one can benefit from it, e.g. by regular discounts.
(for scenario item S2)	q82	Ich meine, auf diese Weise angepasste Preise sind eine gute Sache, da sie gezielter den jeweiligen Personen entsprechen, z.B. könnte man Schülern, Rentnern oder Sozialleistungsempfängern günstigere Preise gewähren.	I think that prices adapted in this way are a good thing, because they better match the needs of the respective person, e.g. one can lower prices for pupils, pensioners, or welfare recipients.
(for scenario item S3)	q83	Ich finde, dass das schwer zu durchschauen wäre.	I think this would be difficult to understand.
(for scenario item S4)	q84	Ich glaube, dass dadurch die Vergleichbarkeit und der Wettbewerb auf Märkten leiden kann.	I believe that the comparability and competition on the markets would suffer from this.
(for scenario item S5)	q85	Ich glaube, dass das Geschäft damit nur seinen Gewinn steigern will.	I believe that the shop would only try to increase its profit.
(for scenario item S6)	q86	Ich würde mich dadurch benachteiligt fühlen, weil es sein könnte, dass ich dann insgesamt mehr bezahle als sonst.	I would feel disadvantaged, because I might finally have to pay more than before.

Scenario 'Retail': Use of data from the internet		Angenommen, das Geschäft würde zur Ermittlung des Kundenprofils und der personalisierten Preise auch auf Daten aus dem Internet, wie z.B. auf Ihre Kommunikation in sozialen Netzwerken oder andere Informationen, die im Internet über Sie ermittelt werden können, zurückgreifen. Bitte geben Sie wieder mit "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu" an, wie Ihre Meinung zu den folgenden Aussagen ist: [Items in zufälliger Reihenfolge]	Assuming the shop would also use data from the internet, e.g. your communication in social networks and other information found about you on the internet, to determine your costumer profile and set personalised prices. Please give your opinion on the following statements on a scale from "1 = fully agree" to "5 = do not agree at all": [Items in random order]
(for scenario item S7)	q8a1	Ich denke, auf diese Weise könnte das Geschäft noch besser mich als Kunden und meine Zahlungsfähigkeit erkennen.	I think in this way the shop could better recognize me as a customer and my solvency.
(for scenario item S8)	q8a2	Ich denke, das wäre ein zu großer Eingriff in die Privatsphäre und sollte verboten sein.	I think this would be too much of an intrusion into privacy and should be prohibited.
(for scenario item S9)	q8a3	Ich glaube, dass dies zu fehleranfällig wäre und man schlecht etwas gegen solche Fehler unternehmen kann.	I believe that this would be too prone to errors and one could hardly take action against such errors.
Feelings about (for scenario item S10)	q8b	Wie fühlen Sie sich insgesamt mit dieser Situation, wenn auf Basis von großen Datenmengen solche Entscheidungen getroffen werden? Bitte geben Sie dies auf einer Skala von "1 = fühle mich sehr wohl damit" bis "5 = fühle mich überhaupt nicht wohl damit" an.	All in all, how do you feel about the situation when decisions are made based on large amounts of data? Please indicate on a scale from "1 = feel very comfortable with it" to "5 = do not feel comfortable with it at all".
Scenario 'Retail': Automated decision-making		In der beschriebenen Situation erfolgt die Auswertung der großen Datenmengen automatisiert durch ein Computersystem. Das Computersystem trifft dann auch die Entscheidung, wie hoch die Preise für Sie sein sollen. Wie stehen Sie zu den folgenden Aussagen? Von „1 = stimme voll und ganz zu" bis „5 = stimme überhaupt nicht zu". [Items in zufälliger Reihenfolge, bis auf letztes]	In the situation described above, a computer system automatically processes the large amounts of data. The computer system also decides about the prices you have to pay. Please give your opinion on the following statements on a scale from "1 = fully agree" to "5 = do not agree at all". [Items in random order, except last one]
(for scenario item S11)	q8c1	Ich glaube, der Computer könnte in diesem Fall bessere Entscheidungen treffen als der Mensch.	I believe in this case the computer could make better decisions than a human.
(for scenario item S12)	q8c2	Ich finde es in Ordnung, dass ein Computer solche Entscheidungen allein und ohne menschliche Kontrolle trifft.	I think it's right that a computer makes such decisions alone and without human control.
(for scenario item S13)	q8c3	Ich meine, der Computer sollte in diesem Fall nur Empfehlungen abgeben und der Mensch sollte immer entscheiden.	I think in this case the computer should only give recommendations and the human should always decide.
(for scenario item S14)	q8c4	Ich finde, es sollte verboten sein, dass Computer in einem solchen Fall Entscheidungen allein treffen. Ein Mensch sollte immer kontrollieren müssen.	I think it should be prohibited that computers make such decisions on their own. A human must always control.
Feelings about (for scenario item S15)	q8d	Wie fühlen Sie sich damit, wenn Computer solche Entscheidungen ohne menschliche Kontrolle treffen würden? Bitte geben Sie dies auf einer Skala von „1 = fühle mich sehr wohl damit" bis „5 = fühle mich sehr unwohl damit" an.	How do you feel about computers making such decisions without human control? Please indicate on a scale from "1 = feel very comfortable with it" to "5 = feel very uncomfortable with it".
Scenario 'Retail': Potential adaptations of behaviour		Wenn das Geschäft auch Daten aus dem Internet nutzen würde, inwieweit träfen dann folgende Aussagen auf Sie zu? Bitte geben Sie dies mit "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu" an:	If the shop also used data from the internet, how far would you agree with the following statements? Please indicate on a scale from "1 = fully agree" to "5 = do not agree at all".
(for scenario item S16)	q8e1	Ich würde mein Verhalten und meine Kommunikation im Internet und bei der Computernutzung nicht ändern.	I would not change my behaviour and my communication on the internet.
(for scenario item S17)	q8e2	Ich würde darauf achten, dass ich nichts Nachteiliges von mir im Internet preisgebe.	I would be careful not to reveal anything negative about me on the internet.
(for scenario item S18)	q8e3	Ich würde z.B. auch Einträge in sozialen Netzwerken oder auf anderen Webseiten bewusst vorteilhaft für mich gestalten.	I would, for instance, make entries in social networks or other websites which put me intentionally in a favourable light.

(for scenario item S19)	q8e4	Ich würde Maßnahmen treffen, um meine Privatsphäre besser zu schützen, z.B. nur noch soziale Netzwerke oder Suchmaschinen benutzen, die dafür bekannt sind, dass sie die Privatsphäre besser schützen.	I would take measures to better protect my privacy, e.g. using only social networks or search engines that are known for better privacy protection.
Scenario 'Retail': Measures requested		Wie Daten vom Geschäft erfasst und verarbeitet werden, könnte auf unterschiedliche Weise erfolgen. Inwieweit stimmen Sie den folgenden Möglichkeiten zu, von "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu": [Items in zufälliger Reihenfolge]	There are different ways the data might be collected and processed by the shop. How far do you agree with the following options on a scale from "1 = fully agree" to "5 = do not agree at all"? [Items in random order]
(for scenario item S20)	q8f1	Ich finde, dass ich einfache Kontrollmöglichkeiten erhalten sollte, welche Daten dabei über mich erhoben werden und wie sie verwendet werden.	I think I should have easy control options over what data about me is collected and how it is used.
(for scenario item S21)	q8f2	Aus meiner Sicht dürfte das Geschäft die Daten an andere Unternehmen weiterverkaufen.	From my point of view, the shop can sell the data to other companies.
(for scenario item S22)	q8f3	Ich finde es in Ordnung, wenn das Geschäft zu Zwecken der Marktforschung die Daten in anonymisierter Form an Dritte weitergeben würde.	It would be fine with me if the shop transferred the data in anonymised form to third parties for purposes of market research.
(for scenario item S23)	q8f4	Ich wünsche mir, dass der Staat gesetzlich regelt und durchsetzt, welche Daten genutzt würden.	I wish that the state would regulate and enforce what data may be used.
Scenario 'Health insurance': Differentiation		Stellen Sie sich eine Situation vor, in der Krankenversicherungen besondere Tarife bieten, wenn man Körperdaten, wie z.B. zur körperlichen Aktivität, kontinuierlich erfassen und von der Krankenkasse auswerten lässt. Die Daten können mit Fitness-Armbändern, speziellen Apps auf Smartphones oder Smartwatches erhoben werden, die mit dem Internet verbunden sind. Bitte geben Sie auf einer Skala von "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu" an, was Sie von den folgenden Aussagen halten: [Items in zufälliger Reihenfolge]	Imagine a situation in which health insurance companies offer special rates if you allow them to continuously collect and analyse your body data, e.g. on physical activities. The data can be collected by fitness trackers, special apps on smartphones or smartwatches that are connected to the internet. Please give your opinion on the following statements on a scale from "1 = fully agree" to "5 = do not agree at all". [Items in random order]
(for scenario item S1)	q91	Ich finde das eine gute Idee, wenn man dadurch Vorteile erhalten kann, wie z.B. einen günstigen Tarif.	I think that is a good idea if one can benefit from it, e.g. by favourable rates.
(for scenario item S2)	q92	Ich meine, solche auf diese Weise angepasste Tarife sind eine gute Sache, da sie gezielter den jeweiligen Personen entsprechen, z.B. entsprechend gesundem oder ungesundem Lebenswandel.	I think that rates adapted in this way are a good thing, because they are tailored to the person's individual situation, e.g. a healthy or unhealthy lifestyle.
(for scenario item S3)	q93	Ich finde, dass das schwer zu durchschauen wäre.	I think this would be difficult to understand.
(for scenario item S4)	q94	Ich glaube, dass dadurch die Solidarität zwischen den Versicherten leiden kann.	I believe that the solidarity among the insurance customers could suffer by this.
(for scenario item S5)	q95	Ich glaube, dass die Versicherung damit nur ihren Gewinn steigern will.	I believe that the insurance company would only try to increase its profit.
(for scenario item S6)	q96	Ich würde mich dadurch benachteiligt fühlen, weil ich schlechtere Tarifkonditionen erhalten könnte.	I would feel disadvantaged because I might get worse rates than before.
Scenario 'Health insurance': Use of data from the internet		Angenommen, die Versicherung würde zur Ermittlung der unterschiedlichen Tarife auch auf Daten aus dem Internet, wie z.B. auf Ihre Kommunikation in sozialen Netzwerken oder andere Informationen, die im Internet über Sie ermittelt werden können, zurückgreifen. Bitte geben Sie mit "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu" an, wie Ihre Meinung zu den folgenden Aussagen ist: [Items in zufälliger Reihenfolge]	Assuming the insurance company would also use data from the internet, e.g. your communication in social networks or other information found about you on the internet, to determine your rate. Please give your opinion on the following statements on a scale from "1 = fully agree" to "5 = do not agree at all": [Items in random order]
(for scenario item S7)	q9a1	Ich denke, auf diese Weise könnte die Versicherung noch besser meine Lebensweise und mich als Versicherten erfassen.	I think, in this way, the insurance company could better understand my lifestyle and me as an insurant.
(for scenario item S8)	q9a2	Ich denke, das wäre ein zu großer Eingriff in die Privatsphäre und sollte verboten sein.	I think this would be too much of an intrusion into privacy and should be prohibited.

(for scenario item S9)	q9a3	Ich glaube, dass dies zu fehleranfällig wäre und man schlecht etwas gegen solche Fehler unternehmen kann.	I believe that this would be too prone to errors and one could hardly take action against such errors.
Feelings about (for scenario item S10)	q9b	Wie fühlen Sie sich insgesamt mit dieser Situation, bei der auf Basis von großen Datenmengen solche Entscheidungen getroffen werden? Bitte geben Sie dies auf einer Skala von 1 = fühle mich sehr wohl damit bis 5 = fühle mich überhaupt nicht wohl damit an.	All in all, how do you feel about the situation when decisions are made based of large amounts of data? Please indicate on a scale from "1 = feel very comfortable about this" to "5 = do not feel comfortable about it at all".
Scenario 'Health insurance': Automated decision-making		In der beschriebenen Situation erfolgt die Auswertung der großen Datenmengen automatisiert durch ein Computersystem. Das Computersystem trifft dann auch die Entscheidung, wie hoch der Tarif für Sie sein soll. Wie stehen Sie zu den folgenden Aussagen? Von "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu". [Items in zufälliger Reihenfolge, bis auf letztes]	In the situation described above, a computer system automatically processes the large amounts of data. The computer system also decides on the rate for you. Please give your opinion on the following statements on a scale from "1 = fully agree" to "5 = do not agree at all": [Items in random order, except last one]
(for scenario item S11)	q9c1	Ich glaube, der Computer könnte in diesem Fall bessere Entscheidungen treffen als der Mensch.	I believe in this case the computer could make better decisions than a human.
(for scenario item S12)	q9c2	Ich finde es in Ordnung, dass ein Computer solche Entscheidungen allein und ohne menschliche Kontrolle trifft.	I think it's right that a computer makes such decisions alone and without human control.
(for scenario item S13)	q9c3	Ich meine, der Computer sollte in diesem Fall nur Empfehlungen abgeben und der Mensch sollte immer entscheiden.	I think in this case the computer should only give recommendations and the human should always decide.
(for scenario item S14)	q9c4	Ich finde, es sollte verboten sein, dass Computer in einem solchen Fall Entscheidungen allein treffen. Ein Mensch sollte immer kontrollieren müssen.	I think it should be prohibited that computers make such decisions on their own. A human must always control.
Feelings about (for scenario item S15)	q9d	Wie fühlen Sie sich damit, wenn Computer solche Entscheidungen ohne menschliche Kontrolle treffen würden? Bitte geben Sie dies auf einer Skala von „1 = fühle mich sehr wohl damit" bis „5 = fühle mich sehr unwohl damit" an.	How do you feel about computers making such decisions without human control? Please indicate on a scale from "1 = feel very comfortable with it" to "5 = feel very uncomfortable with it".
Scenario 'Health insurance': Potential adaptations of behaviour		Wenn die Versicherung auch Daten aus dem Internet nutzen würde, inwieweit träfen dann folgende Aussagen auf Sie zu? Bitte geben Sie dies mit "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu" an:	If the insurance company also use data from the internet, how far would you agree with the following statements? Please indicate on a scale from "1 = fully agree" to "5 = do not agree at all".
(for scenario item S16)	q9e1	Ich würde mein Verhalten und meine Kommunikation im Internet und bei der Computernutzung nicht ändern.	I would not change my behaviour and my communication on the internet.
(for scenario item S17)	q9e2	Ich würde darauf achten, dass ich nichts Nachteiliges von mir im Internet preisgebe.	I would be careful not to reveal anything negative about me on the internet.
(for scenario item S18)	q9e3	Ich würde z.B. auch Einträge in sozialen Netzwerken oder auf anderen Webseiten bewusst vorteilhaft für mich gestalten.	I would, for instance, make entries in social networks or other websites which put me intentionally in a favourable light.
(for scenario item S19)	q9e4	Ich würde Maßnahmen treffen, um meine Privatsphäre besser zu schützen, z.B. nur noch soziale Netzwerke oder Suchmaschinen benutzen, die dafür bekannt sind, dass sie die Privatsphäre besser schützen.	I would take measures to better protect my privacy, e.g. using only social networks or search engines that are known for better privacy protection.
Scenario 'Health insurance': Measures requested		Wie Daten von der Versicherung erfasst und verarbeitet werden, könnte auf unterschiedliche Weise erfolgen. Inwieweit stimmen Sie den folgenden Möglichkeiten zu, von "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu": [Items in zufälliger Reihenfolge]	There are different ways the data might be collected and processed by the insurance company. How far do you agree with the following options on a scale from "1 = fully agree" to "5 = do not agree at all"? [Items in random order]
(for scenario item S20)	q9f1	Ich finde, dass ich einfache Kontrollmöglichkeiten erhalten sollte, welche Daten dabei über mich erhoben werden und wie sie verwendet werden.	I think I should have easy control options over what data about me is collected and how it is used.

(for scenario item S21)	q9f2	Aus meiner Sicht dürfte die Versicherung die Daten an andere Unternehmen weiterverkaufen.	From my point of view, the insurance company can sell the data to other companies.
(for scenario item S22)	q9f3	Ich finde es in Ordnung, wenn die Versicherung zu Zwecken der medizinischen Forschung die Daten in anonymisierter Form an Dritte weitergeben würde.	It would be fine with me if the insurance company transferred the data in anonymised form to third parties for purposes of market research.
(for scenario item S23)	q9f4	Ich wünsche mir, dass der Staat gesetzlich regelt und durchsetzt, welche Daten genutzt würden.	I wish that the state would regulate and enforce what data may be used.

Scenario 'Credit': Differentiation		Stellen Sie Sich nun eine andere Situation vor. Sie wollen einen Kredit bei einer Bank aufnehmen. Üblicherweise werden dazu ihre Einkommens- und Vermögensverhältnisse geprüft. Stellen Sie sich nun vor, das zusätzlich auch Informationen über Ihren Zahlungsverkehr, also was sie gekauft und wofür sie bezahlt haben, ausgewertet werden. Auf Grundlage dieser Daten wird dann die Entscheidung über die Gewährung des Kredits getroffen und die Konditionen festgelegt. Bitte geben Sie auf einer Skala von "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu" an, was Sie von den folgenden Aussagen halten: [Items in zufälliger Reihenfolge]	Now imagine a different situation. You want to obtain a loan from a bank. Usually, the bank will examine your income and financial circumstances. Imagine that, in addition, it would also examine information about your payments, i.e. what you have bought and what you paid for. Based on this, decisions will be made about credit granting and credit terms. Please indicate on a scale from "1 = fully agree" to "5 = do not agree at all" what do you think about the following statements. [Items in random order]
(for scenario item S1)	q101	Ich finde das eine gute Idee, wenn man dadurch Vorteile erhalten kann, wie einen günstigen Kredit.	I think that is a good idea if I can benefit from it, e.g. by cheaper credit.
(for scenario item S2)	q102	Ich meine, auf diese Weise angepasste Kreditentscheidungen und Kreditkonditionen sind eine gute Sache, da sie gezielter den jeweiligen Personen entsprechen, z.B. der Kreditwürdigkeit oder den Rückzahlungsmöglichkeiten der Person.	I think that credit decisions and terms adapted in this way are a good thing, because they are tailored to persons' individual situation, e.g. the creditworthiness or the repayment ability of the person.
(for scenario item S3)	q103	Ich finde, dass das schwer zu durchschauen wäre.	I think this would be difficult to understand.
(for scenario item S4)	q104	Ich glaube, dass dadurch die Vergleichbarkeit der Kreditangebote und der Wettbewerb zwischen den Banken erschwert werden könnte.	I believe that the comparability of credit offers and the competition between banks could become more difficult.
(for scenario item S5)	q105	Ich glaube, dass die Bank damit nur ihren Gewinn steigern will.	I believe that the bank would only try to increase its profit with it.
(for scenario item S6)	q106	Ich würde mich dadurch benachteiligt fühlen, weil ich schlechtere Kreditkonditionen erhalten könnte.	I would feel disadvantaged because I might get worse credit terms than before.
Scenario 'Credit': Use of data from the internet		Angenommen, die Bank würde zur Ermittlung der Kreditkonditionen auch auf Daten aus dem Internet, wie z.B. auf Ihre Kommunikation in sozialen Netzwerken oder andere Informationen, die im Internet über Sie ermittelt werden können, zurückgreifen. Bitte geben Sie mit "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu" an, wie Ihre Meinung zu den folgenden Aussagen ist: [Items in zufälliger Reihenfolge]	Assuming the bank would also use data from the internet, e.g. your communication in social networks and other information found about you on the internet, to determine the credit terms. Please give your opinion on the following statements on a scale from "1 = fully agree" to "5 = do not agree at all": [Items in random order]
(for scenario item S7)	q10a1	Ich denke, auf diese Weise könnte die Bank noch besser meine Lebensweise und mich als Kreditnehmer erfassen.	I think in this way the bank could better understand my lifestyle and me as a borrower.
(for scenario item S8)	q10a2	Ich denke, das wäre ein zu großer Eingriff in die Privatsphäre und sollte verboten sein.	I think this would be too much of an intrusion into privacy and should be prohibited.
(for scenario item S9)	q10a3	Ich glaube, dass dies zu fehleranfällig wäre und man schlecht etwas gegen solche Fehler unternehmen kann.	I believe that this would be too prone to errors and one could hardly take action against such errors.
Feelings about (for scenario item S10)	q10b	Wie fühlen Sie sich insgesamt mit dieser Situation, bei der auf Basis von großen Datenmengen solche Entscheidungen getroffen werden? Bitte geben Sie dies auf einer Skala von "1 = fühle mich sehr wohl damit" bis "5 = fühle mich überhaupt nicht wohl damit" an.	All in all, how do you feel about the situation when decisions are made based on large amounts of data? Please indicate this on a scale from "1 = feel very comfortable about this" to "5 = do not feel comfortable about it at all".

Scenario 'Credit': Automated decision-making		In der beschriebenen Situation erfolgt die Auswertung der großen Datenmengen automatisiert durch ein Computersystem. Das Computersystem trifft dann auch die Entscheidung über die Gewährung des Kredits und über die Konditionen. Wie stehen Sie zu den folgenden Aussagen? Von "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu". [Items in zufälliger Reihenfolge, bis auf letztes]	In the situation described above, a computer system automatically processes the large amounts of data. The computer system also decides on credit granting and credit terms. Please give your opinion on the following statements on a scale from "1 = fully agree" to "5 = do not agree at all": [Items in random order, except last one]
(for scenario item S11)	q10c1	Ich glaube, der Computer könnte in diesem Fall bessere Entscheidungen treffen als der Mensch.	I believe in this case the computer could make better decisions than a human.
(for scenario item S12)	q10c2	Ich finde es in Ordnung, dass ein Computer solche Entscheidungen allein und ohne menschliche Kontrolle trifft.	I think it's right that a computer makes such decisions alone and without human control.
(for scenario item S13)	q10c3	Ich meine, der Computer sollte in diesem Fall nur Empfehlungen abgeben und der Mensch sollte immer entscheiden.	I think in this case the computer should only give recommendations and the human should always decide.
(for scenario item S14)	q10c4	Ich finde, es sollte verboten sein, dass Computer in einem solchen Fall Entscheidungen allein treffen. Ein Mensch sollte immer kontrollieren müssen.	I think it should be prohibited that computers make such decisions on their own. A human must always control.
Feelings about (for scenario item S15)	q10d	Wie fühlen Sie sich damit, wenn Computer solche Entscheidungen ohne menschliche Kontrolle treffen würden? Bitte geben Sie dies auf einer Skala von „1 = fühle mich sehr wohl damit" bis „5 = fühle mich sehr unwohl damit" an.	How do you feel about computers making such decisions without human control? Please indicate on a scale from "1 = feel very comfortable with it" to "5 = feel very uncomfortable with it".
Scenario 'Credit': Potential adaptations of behaviour		Wenn die Bank auch Daten aus dem Internet nutzen würde, inwieweit träfen dann folgende Aussagen auf Sie zu? Bitte geben Sie dies mit "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu" an:	If the bank also uses data from the internet, how far would you agree with the following statements? Please indicate on a scale from "1 = fully agree" to "5 = do not agree at all".
(for scenario item S16)	q10e1	Ich würde mein Verhalten und meine Kommunikation im Internet und bei der Computernutzung nicht ändern.	I would not change my behaviour and my communication on the internet.
(for scenario item S17)	q10e2	Ich würde darauf achten, dass ich nichts Nachteiliges von mir im Internet preisgebe.	I would be careful not to reveal anything negative about me on the internet.
(for scenario item S18)	q10e3	Ich würde z.B. auch meine Einträge in sozialen Netzwerken bewusst vorteilhaft für mich gestalten.	I would, for instance, make entries in social networks or other websites which put me intentionally in a favourable light.
(for scenario item S19)	q10e4	Ich würde Maßnahmen treffen, um meine Privatsphäre besser zu schützen, z.B. nur noch soziale Netzwerke oder Suchmaschinen benutzen, die dafür bekannt sind, dass sie die Privatsphäre besser schützen.	I would take measures to better protect my privacy, e.g. using only social networks or search engines that are known for better privacy protection.
Scenario 'Credit': Measures requested		Wie Daten von der Bank erfasst und verarbeitet werden, könnte auf unterschiedliche Weise erfolgen. Inwieweit stimmen Sie den folgenden Möglichkeiten zu, von "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu": [Items in zufälliger Reihenfolge]	There are different ways the data might be collected and processed by the bank. How far do you agree with the following options on a scale from "1 = fully agree" to "5 = do not agree at all"? [Items in random order]
(for scenario item S20)	q10f1	Ich finde, dass ich einfache Kontrollmöglichkeiten erhalten sollte, welche Daten dabei über mich erhoben werden und wie sie verwendet werden.	I think I should have easy control options over what data about me is collected and how it is used.
(for scenario item S21)	q10f2	Aus meiner Sicht dürfte die Bank die Daten an andere Unternehmen weiterverkaufen.	From my point of view, the bank can sell the data to other companies.
(for scenario item S22)	q10f3	Ich finde es in Ordnung, wenn die Bank zu Zwecken der Marktforschung die Daten in anonymisierter Form an Dritte weitergeben würde.	It would be fine with me if the bank transferred the data in anonymised form to third parties for purposes of market research.
(for scenario item S23)	q10f4	Ich wünsche mir, dass der Staat gesetzlich regelt und durchsetzt, welche Daten genutzt würden.	I wish that the state would regulate and enforce what data may be used.

Scenario ‘Employment’: Differentiation		Stellen Sie sich nun eine andere Situation vor. Sie sind in einem Büro angestellt und arbeiten dort viel mit dem Computer. Dabei würden Ihre Aktivitäten, z.B. wie schnell Sie E-Mails beantworten oder wie schnell Sie tippen oder was sie in den E-Mails schreiben, durch den Arbeitgeber erfasst und ausgewertet. Auf Grundlage dieser Daten wird dann über die Entlohnung und die Arbeitsbedingungen entschieden. Bitte geben Sie auf einer Skala von "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu" an, was Sie von den folgenden Aussagen halten: [Items in zufälliger Reihenfolge]	Now imagine a different situation. You work in an office where you often use the computer. In doing so, your activities, e.g. how fast you answer emails, how fast you type, or what you write in the emails, would be recorded and analysed by the employer. Decisions about your wages and working conditions are then based on this data. Please indicate on a scale from "1 = fully agree" to "5 = do not agree at all" how much you agree with the following statements. [Items in random order]
(for scenario item S1)	q111	Ich finde das eine gute Idee, wenn man dadurch Vorteile erhalten kann, insbesondere, dass man besser beurteilt werden kann.	I think that is a good idea, if I can benefit from it, in particular, by being better appraised.
(for scenario item S2)	q112	Ich meine, unterschiedliche Entlohnung und Arbeitsbedingungen sind eine gute Sache, da sie gezielter den jeweiligen Personen entsprechen, z.B. hinsichtlich der Arbeitserfahrung und Qualifikation.	I believe that differentiated wages and working conditions are a good thing, because they are tailored to the individual person, e.g. regarding work experiences and qualification.
(for scenario item S3)	q113	Ich finde, dass das schwer zu durchschauen wäre.	I think this would be difficult to understand.
(for scenario item S4)	q114	Ich glaube, dass damit die Leistungen besser beurteilt werden könnten.	I believe that the employees' performance could be better assessed.
(for scenario item S5)	q115	Ich glaube, dass der Arbeitgeber damit nur die Entlohnung gering halten will.	I believe that the employer would only try to keep wages low.
(for scenario item S6)	q116	Ich würde mich dadurch benachteiligt fühlen, weil ich schlechtere Entlohnung und Arbeitsbedingungen erhalten könnte.	I would feel disadvantaged because I might get worse wages and working conditions than before.
Scenario ‘Employment’: Use of data from the internet		Angenommen, der Arbeitgeber würde für Entscheidungen über Entlohnung und Arbeitsbedingungen auch auf Daten aus dem Internet, wie z.B. auf Ihre Kommunikation in sozialen Netzwerken oder andere Informationen, die im Internet über Sie ermittelt werden können, zurückgreifen. Bitte geben Sie mit "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu" an, wie Ihre Meinung zu den folgenden Aussagen ist: [Items in zufälliger Reihenfolge]	Assuming the employer would also use data from the internet, e.g. your communication in social networks and other information found about you on the internet, to make decisions on wages and working conditions. Please give your opinion on the following statements on a scale from "1 = fully agree" to "5 = do not agree at all". [Items in random order]
(for scenario item S7)	q11a1	Ich denke, auf diese Weise könnte der Arbeitgeber noch besser meine Leistungsfähigkeit und mich als Arbeitnehmer erfassen.	I think in this way the employer could better access my performance and me as an employee.
(for scenario item S8)	q11a2	Ich denke, das wäre ein zu großer Eingriff in die Privatsphäre und sollte verboten sein.	I think this would be too much of an intrusion into privacy and should be prohibited.
(for scenario item S9)	q11a3	Ich glaube, dass dies zu fehleranfällig wäre und man schlecht etwas gegen solche Fehler unternehmen kann.	I believe that this would be too prone to errors and one could hardly take action against such errors.
Feelings about (for scenario item S10)	q11b	Wie fühlen Sie sich insgesamt mit dieser Situation, bei der auf Basis von großen Datenmengen solche Entscheidungen getroffen werden? Bitte geben Sie dies auf einer Skala von "1 = fühle mich sehr wohl damit" bis "5 = fühle mich überhaupt nicht wohl damit" an.	All in all, how do you feel about this situation when decisions are made on the base of large volumes of data? Please indicate on a scale from "1 = feel very comfortable about this" to "5 = do not feel comfortable about it at all".
Scenario ‘Employment’: Automated decision-making		In der beschriebenen Situation erfolgt die Auswertung der großen Datenmengen automatisiert durch ein Computersystem. Das Computersystem trifft dann auch die Entscheidung über die Entlohnung und die Arbeitsbedingungen. Wie stehen Sie zu den folgenden Aussagen? Von "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu". [Items in zufälliger Reihenfolge, bis auf letztes]	In the situation described above, a computer system automatically processes the large amounts of data. The computer system also decides on the wages and working conditions. Please give your opinion on the following statements on a scale from "1 = fully agree" to "5 = do not agree at all": [Items in random order, except last one]
(for scenario item S11)	q11c1	Ich glaube, der Computer könnte in diesem Fall bessere Entscheidungen treffen als der Mensch.	I believe in this case the computer could make better decisions than a human.

(for scenario item S12)	q11c2	Ich finde es in Ordnung, dass ein Computer solche Entscheidungen allein und ohne menschliche Kontrolle trifft.	I think it's right that a computer makes such decisions alone and without human control.
(for scenario item S13)	q11c3	Ich meine, der Computer sollte in diesem Fall nur Empfehlungen abgeben und der Mensch sollte immer entscheiden.	I think in this case the computer should only give recommendations and the human should always decide.
(for scenario item S14)	q11c4	Ich finde, es sollte verboten sein, dass Computer in einem solchen Fall Entscheidungen allein treffen. Ein Mensch sollte immer kontrollieren müssen.	I think it should be prohibited that computers make such decisions on their own. A human must always control.
Feelings about (for scenario item S15)	q11d	Wie fühlen Sie sich damit, wenn Computer solche Entscheidungen ohne menschliche Kontrolle treffen würden? Bitte geben Sie dies auf einer Skala von "1 = fühle mich sehr wohl damit" bis "5 = fühle mich sehr unwohl damit" an.	How do you feel about computers making such decisions without human control? Please indicate on a scale from "1 = feel very comfortable with it" to "5 = feel very uncomfortable with it".
Scenario 'Employment': Potential adaptations of behaviour		Wenn der Arbeitgeber auch Daten aus dem Internet nutzen würde, inwieweit träfen dann folgende Aussagen auf Sie zu? Bitte geben Sie dies mit "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu" an.	If the employer also used data from the internet, how far would you agree with the following statements? Please indicate on a scale from "1 = fully agree" to "5 = do not agree at all".
(for scenario item S16)	q11e1	Ich würde mein Verhalten und meine Kommunikation im Internet und bei der Computernutzung nicht ändern.	I would not change my behaviour and my communication on the internet.
(for scenario item S17)	q11e2	Ich würde darauf achten, dass ich nichts Nachteiliges von mir im Internet preisgebe.	I would be careful not to reveal anything negative about me on the internet.
(for scenario item S18)	q11e3	Ich würde z.B. auch meine Einträge in sozialen Netzwerken bewusst vorteilhaft für mich gestalten.	I would, for instance, make entries in social networks or other websites which put me intentionally in a favourable light.
(for scenario item S19)	q11e4	Ich würde Maßnahmen treffen, um meine Privatsphäre besser zu schützen, z.B. nur noch soziale Netzwerke oder Suchmaschinen benutzen, die dafür bekannt sind, dass sie die Privatsphäre besser schützen.	I would take measures to better protect my privacy, e.g. using only social networks or search engines that are known for better privacy protection.
Scenario 'Employment': measures requested		Wie Daten vom Arbeitgeber erfasst und verarbeitet werden, könnte auf unterschiedliche Weise erfolgen. Inwieweit stimmen Sie den folgenden Möglichkeiten zu, von "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu"? [Items in zufälliger Reihenfolge]	There are different ways the data might be collected and processed by the employer. How far do you agree with the following options on a scale from "1 = fully agree" to "5 = do not agree at all"? [Items in random order]
(for scenario item S20)	q11f1	Ich finde, dass ich einfache Kontrollmöglichkeiten erhalten sollte, welche Daten dabei über mich erhoben werden und wie sie verwendet werden.	I think I should have easy control options over what data about me is collected and how it is used.
(for scenario item S21)	q11f2	Aus meiner Sicht dürfte der Arbeitgeber die Daten an andere Unternehmen weiterverkaufen.	From my point of view, the employer can sell the data to other companies.
(for scenario item S22)	q11f3	Ich finde es in Ordnung, wenn der Arbeitgeber zu Zwecken der Arbeitsmarktforschung die Daten in anonymisierter Form an Dritte weitergeben würde.	It would be fine with me if the employer transferred the data in anonymised form to third parties for purposes of labour market research.
(for scenario item S23)	q11f4	Ich wünsche mir, dass der Staat gesetzlich regelt und durchsetzt, welche Daten genutzt würden.	I wish that the state would regulate and enforce what data may be used.

Institutional framework on privacy and data protection

Privacy policy		Bevor man ein Angebot im Internet oder ein vernetztes Gerät nutzen möchte, wird man in der Regel nach der Zustimmung zur Datenschutzerklärung gefragt. Sie wird auch manchmal als Datenschutzrichtlinie oder "Privacy Policy" bezeichnet.	Before using an offer on the internet or a connected device, you are usually asked to consent to the privacy statement (Datenschutzerklärung). The privacy statement is sometimes also called privacy policy.
Reading	q12	Wie häufig lesen Sie sich Datenschutzerklärungen zumindest teilweise durch? [Antwortmöglichkeiten:] Immer; Oft; Manchmal; Selten; Nie	How often do you read the privacy policies at least partially? [Options to answer:] Always; Often; Sometimes; Rarely; Never

Understanding	q13	Wenn Sie die Datenschutzerklärungen gelesen haben, wie oft hatten Sie das Gefühl, sie weitestgehend verstanden zu haben? [Antwortmöglichkeiten:] Immer; Oft; Manchmal; Selten; Nie	If you have read the privacy policies how often do you feel that you have largely understood them? [Options to answer:] Always; Often; Sometimes; Rarely; Never
Improvements requested	q14	Welche Maßnahmen würden Sie sich wünschen, die Ihnen bei den Datenschutzerklärungen helfen könnten? Sie können zu mehreren Maßnahmen ja oder nein angeben. [Items in zufälliger Reihenfolge]	What measures would you like to see introduced to support you with privacy policies? You can answer yes or no to multiple measures. [Items in random order]
	q14_01	Einfache Symbole, die über die Arten des Umgangs mit Daten informieren	Simple symbols that inform about the types of data use
	q14_02	Eine einfache und klare Sprache, die jeder verstehen kann	A simple and clear language that everyone can understand
	q14_03	Datenschutz- und Verbraucherschutzorganisationen sollten die Datenschutzerklärungen prüfen und bei Missbrauch dagegen vorgehen	Data and consumer protection organisations should examine the privacy policies and take action against misuse.
	q14_04	Datenschutzerklärungen sollten von staatlichen Stellen geprüft und Missbrauch sollte bestraft werden	Privacy policies should be examined by governmental agencies, and misuse should be punished.
	q14_05	weitere Hinweise (notiert)	further comments (noted)
Purpose limitations and trust		Angenommen, Sie hätten der Datenschutzerklärung und den darin beschriebenen Zwecken der Datenverarbeitung durch ein Unternehmen eingewilligt, inwieweit würden Sie den nachfolgenden Aussagen zustimmen? Von "1 = stimme voll und ganz zu" bis "5 = stimme überhaupt nicht zu". [Items in zufälliger Reihenfolge]	Assuming you consented to a company's privacy policies and data processing purposes described therein. How far do you agree with the following statements on a scale from "1 = fully agree" to "5 = do not agree at all"? [Items in random order]
	q151	Ich glaube, dass Unternehmen sich an die beschriebenen Zwecke der Datenverarbeitung halten und sonst nichts anderes mit den Daten machen.	I believe that companies adhere to the data processing purposes described in their policies and do nothing else with the data.
	q152	Ich finde, von Unternehmen erfährt man klar und vollständig, welche Daten über mich verarbeitet werden.	I think companies clearly and comprehensively inform me of what data about me are being processed.
	q153	Ich glaube, Unternehmen fragen mich immer, wenn Daten für andere Zwecke verwendet werden.	I think companies always ask me when data are used for other purposes.
	q154	Ich glaube, Unternehmen fragen mich immer, wenn Daten an Dritte weitergegeben werden.	I think companies always ask me when data are transferred to third parties.
	q155	Ich meine, dass Unternehmen nicht ehrlich sind, wenn es um die Nutzung von Daten über mich geht.	I believe that companies are not honest when it comes to using data about me.
	q156	Ich glaube, dass von mir neue Daten erstellt werden, ohne dass ich das weiß oder dem zugestimmt habe.	I believe that new data about me are generated without my knowing or having consented to it.
Demands on institutional framework of data protection		Zum Thema Datenschutz lese ich Ihnen ein paar Aussagen vor und würde Sie bitten, kurz mit "Ja" oder "Nein" zu antworten, je nachdem, ob Sie der Aussage zustimmen oder nicht. [Items in zufälliger Reihenfolge; Mehrfachantworten möglich.]	I would like to read you a few statements on the subject of data protection and ask you to briefly answer them with "yes" or "no" depending on whether you agree with the statement or not. [Items in random order. Multiple answers possible.]
	q161	Es ist ausschließlich jeder selbst für den Schutz seiner Daten verantwortlich.	Everyone is solely responsible for protecting their data.
	q162	Ich weiß, wohin ich mich wenden kann, um meine Datenschutzrechte durchzusetzen.	I know whom to contact in order to enforce my data protection rights.
	q163	Ich wünsche mir allgemein mehr Informationen und Bildungsmaßnahmen über die Chancen und Risiken der Datenverarbeitung und wie man damit umgehen kann.	I generally want better information and education about the opportunities and risks of data processing and how to deal with them.
	q164	Ich würde gern viel mehr über Computer, Internet und Datenschutz lernen.	I would like to learn much more about computers, the internet, and data protection.

	q165	Ich fände es gut, wenn bereits Kinder und Jugendliche in der Schule über die Chancen und Risiken der Datenverarbeitung unterrichtet werden.	I would like to see children and young people being taught about the opportunities and risks of data processing already in school.
	q166	Ich fände es gut, wenn Verbraucher- und Datenschutzorganisationen mehr gegen Datenmissbräuche vorgehen würden.	I think it would be good if consumer and data protection organisations took more action against misuse of data.
	q167	Die bestehenden Datenschutzgesetze sollten besser durchgesetzt werden.	The existing data protection laws should be better enforced.
	q168	Es sollte mehr staatliche Überprüfungen geben, die dafür sorgen, dass möglichst wenig Daten über mich gesammelt werden.	There should be more government investigations to ensure that as few data as possible are collected about me.
	q169	Der Staat sollte gesetzlich und mit nötigen Vorkehrungen dafür sorgen, dass ich immer weiß, welche Daten über mich verarbeitet werden.	The government should regulate by law and ensure by necessary precautions that I always know what data about me are processed.
	q1610	Der Staat sollte härtere Strafen bei Missbräuchen mit Daten über Personen erlassen.	The government should impose harsher penalties for misuses of personal data.
	q1611	Es sollte besser kontrolliert und geregelt werden, wie international Daten ausgetauscht werden.	The international transfer of data should be better controlled and regulated.
Right to access	q17	Haben Sie schon einmal davon gehört, dass Sie ein Recht darauf haben, bei einem Unternehmen oder einer Behörde nachzufragen, welche Daten über Sie verarbeitet werden? [Antwortmöglichkeit:] Ja; Nein	Have you ever heard that you have a right to ask a company or an authority for information about the data they process about you? [Options to answer:] Yes; No
	q17a	Haben Sie schon einmal diese Möglichkeit genutzt und bei einem Unternehmen oder bei einer Behörde nachgefragt, welche Daten über Sie verarbeitet werden? [Antwortmöglichkeit:] Ja; Nein	Have you ever used this option and asked a company or an authority for information about what data they process about you? [Options to answer:] Yes; No
Right to correction and erasure	q18	Haben Sie schon einmal davon gehört, dass Sie ein Recht darauf haben, die Änderung von falschen Daten oder die Löschung von bestimmten Daten über Sie zu beantragen? [Antwortmöglichkeit:] Ja; Nein	Have you ever heard that you have a right to request correction of incorrect data or erasure of certain data about you? [Options to answer:] Yes; No
	q18a	Haben Sie schon einmal diese Möglichkeit genutzt und die Änderung oder Löschung von Daten über Sie beantragt? [Antwortmöglichkeit:] Ja; Nein	Have you ever used this option and requested correction or erasure of data about you? [Options to answer:] Yes; No

Term ‘big data’

Knowledge about the term	q19	Unabhängig von unserem heutigen Gespräch, haben Sie schon einmal von dem Begriff 'Big Data' gehört? [Antwortmöglichkeiten:] Ja; Nein	Have you ever heard of the term "big data" before our conversation today? [Options to answer:] Yes; No
Associations with the term	q19a	Denken Sie, dass sich für die gesamte Gesellschaft mit 'Big Data' eher mehr Vorteile oder mehr Nachteile ergeben? [Antwortmöglichkeiten:] Eher mehr Vorteile; Eher mehr Nachteile; Kann mich nicht entscheiden; weiß nicht; keine Angabe	Do you think that 'big data' will bring more advantages or more disadvantages for society? [Options to answer:] Expecting more advantages; Expecting more disadvantages; Can not decide; Don’t know; Not specified

Personal Value Questionnaire (PVQ)

PVQ, female		Wir kommen nun zu Fragen, die dem Forschungsprojekt helfen, die Wertevorstellung der Bevölkerung zu verstehen und wie verschiedene Personentypen mit bestimmten Wertevorstellungen sich im Umgang mit Daten entscheiden würden. Ich lese Ihnen dazu im Folgenden kurze Personenbeschreibungen vor und frage Sie "Wie ähnlich ist Ihnen diese Person?". Bitte geben Sie dies auf einer Skala von 1 für "sehr ähnlich" bis 6 für "sehr unähnlich" an.	We now come to questions that will help the research project understand the values of the population and how different types of persons with certain values would decide about the handling of data. I will read you short descriptions of persons and ask you "How much is this person like you?" Please indicate on a scale from 1 for "Very much like me" to 6 for "Not like me at all".
	q201	Es ist ihr wichtig, neue Ideen zu entwickeln und kreativ zu sein. Sie macht Sachen gerne auf ihre eigene originelle Art und Weise.	Thinking up new ideas and being creative is important to her. She likes to do things in her own original way.
	q202	Es ist ihr wichtig, reich zu sein. Sie möchte viel Geld haben und teure Sachen besitzen.	It is important to her to be rich. She wants to have a lot of money and expensive things.
	q203	Sie hält es für wichtig, dass alle Menschen auf der Welt gleich behandelt werden sollten. Sie glaubt, dass jeder Mensch im Leben gleiche Chancen haben sollte.	She thinks it is important that every person in the world should be treated equally. She believes everyone should have equal opportunities in life.
	q204	Es ist ihr wichtig, ihre Fähigkeiten zu zeigen. Sie möchte, dass die Leute bewundern, was sie tut.	It's important to her to show her abilities. She wants people to admire what she does.
	q205	Es ist ihr wichtig, in einem sicheren Umfeld zu leben. Sie vermeidet alles, was ihre Sicherheit gefährden könnte.	It is important to her to live in secure surroundings. She avoids anything that might endanger her safety.
	q206	Sie mag Überraschungen und hält immer Ausschau nach neuen Aktivitäten. Sie denkt, dass im Leben Abwechslung wichtig ist.	She likes surprises and is always looking for new things to do. She thinks it is important to do lots of different things in life.
	q207	Sie glaubt, dass die Menschen tun sollten, was man ihnen sagt. Sie denkt, dass Menschen sich immer an Regeln halten sollten, selbst dann, wenn es niemand sieht.	She believes that people should do what they are told. She thinks people should follow rules at all times, even when no-one is watching.
	q208	Es ist ihr wichtig, Menschen zuzuhören, die anders sind als sie. Auch wenn sie anderer Meinung ist als andere, will sie sie trotzdem verstehen.	It is important to her to listen to people who are different from her. Even when she disagrees with them, she still wants to understand them.
	q209	Es ist ihr wichtig, zurückhaltend und bescheiden zu sein. Sie versucht, die Aufmerksamkeit nicht auf sich zu lenken.	It is important to her to be humble and modest. She tries not to draw attention to herself.
	q2010	Es ist ihr wichtig, Spaß zu haben. Sie gönnt sich selbst gerne etwas.	Having a good time is important to her. She likes to "spoil" herself.
	q2011	Es ist ihr wichtig, selbst zu entscheiden, was sie tut. Sie ist gerne frei und unabhängig von anderen.	It is important to her to make her own decisions about what she does. She likes to be free and not depend on others.
	q2012	Es ist ihr sehr wichtig, den Menschen um sie herum zu helfen. Sie will für deren Wohl sorgen.	It's very important to her to help the people around her. She wants to care for their well-being.
	q2013	Es ist ihr wichtig, sehr erfolgreich zu sein. Sie hofft, dass die Leute ihre Leistungen anerkennen.	Being very successful is important to her. She hopes people will recognise her achievements.
	q2014	Es ist ihr wichtig, dass der Staat ihre persönliche Sicherheit vor allen Bedrohungen gewährleistet. Sie will einen starken Staat, der seine Bürger verteidigt.	It is important to her that the government ensures her safety against all threats. She wants the state to be strong so it can defend its citizens.
	q2015	Sie sucht das Abenteuer und geht gerne Risiken ein. Sie will ein aufregendes Leben haben.	She looks for adventures and likes to take risks. She wants to have an exciting life.
	q2016	Es ist ihr wichtig, sich jederzeit korrekt zu verhalten. Sie vermeidet es, Dinge zu tun, die andere Leute für falsch halten könnten.	It is important to her always to behave properly. She wants to avoid doing anything people would say is wrong.
	q2017	Es ist ihr wichtig, dass andere sie respektieren. Sie will, dass die Leute tun, was sie sagt.	It is important to her to get respect from others. She wants people to do what she says.
	q2018	Es ist ihr wichtig, ihren Freunden gegenüber loyal zu sein. Sie will sich für Menschen einsetzen, die ihr nahe stehen.	It is important to her to be loyal to her friends. She wants to devote herself to people close to her.

	q2019	Sie ist fest davon überzeugt, dass die Menschen sich um die Natur kümmern sollten. Umweltschutz ist ihr wichtig.	She strongly believes that people should care for nature. Looking after the environment is important to her.
	q2020	Tradition ist ihr wichtig. Sie versucht, sich an die Sitten und Gebräuche zu halten, die ihr von ihrer Religion oder ihrer Familie überliefert wurden.	Tradition is important to her. She tries to follow the customs handed down by her religion or her family.
	q2021	Sie lässt keine Gelegenheit aus, Spaß zu haben. Es ist ihr wichtig, Dinge zu tun, die ihr Vergnügen bereiten.	She seeks every chance she can to have fun. It is important to her to do things that give her pleasure.
PVQ, male	q211	Es ist ihm wichtig, neue Ideen zu entwickeln und kreativ zu sein. Er macht Sachen gerne auf seine eigene originelle Art und Weise.	Thinking up new ideas and being creative is important to him. He likes to do things in his own original way.
	q212	Es ist ihm wichtig, reich zu sein. Er möchte viel Geld haben und teure Sachen besitzen.	It is important to him to be rich. He wants to have a lot of money and expensive things.
	q213	Er hält es für wichtig, dass alle Menschen auf der Welt gleich behandelt werden sollten. Er glaubt, dass jeder Mensch im Leben gleiche Chancen haben sollte.	He thinks it is important that every person in the world should be treated equally. He believes everyone should have equal opportunities in life.
	q214	Es ist ihm wichtig, seine Fähigkeiten zu zeigen. Er möchte, dass die Leute bewundern, was er tut.	It's important to him to show his abilities. He wants people to admire what he does.
	q215	Es ist ihm wichtig, in einem sicheren Umfeld zu leben. Er vermeidet alles, was seine Sicherheit gefährden könnte.	It is important to him to live in secure surroundings. He avoids anything that might endanger his safety.
	q216	Er mag Überraschungen und hält immer Ausschau nach neuen Aktivitäten. Er denkt, dass im Leben Abwechslung wichtig ist.	He likes surprises and is always looking for new things to do. He thinks it is important to do lots of different things in life.
	q217	Er glaubt, dass die Menschen tun sollten, was man ihnen sagt. Er denkt, dass Menschen sich immer an Regeln halten sollten, selbst dann, wenn es niemand sieht.	He believes that people should do what they are told. He thinks people should follow rules at all times, even when no-one is watching.
	q218	Es ist ihm wichtig, Menschen zuzuhören, die anders sind als er. Auch wenn er anderer Meinung ist als andere, will er sie trotzdem verstehen.	It is important to him to listen to people who are different from him. Even when he disagrees with them, he still wants to understand them.
	q219	Es ist ihm wichtig, zurückhaltend und bescheiden zu sein. Er versucht, die Aufmerksamkeit nicht auf sich zu lenken.	It is important to him to be humble and modest. He tries not to draw attention to himself.
	q2110	Es ist ihm wichtig, Spaß zu haben. Er gönnt sich selbst gerne etwas.	Having a good time is important to him. He likes to "spoil" himself.
	q2111	Es ist ihm wichtig, selbst zu entscheiden, was er tut. Er ist gerne frei und unabhängig von anderen.	It is important to him to make his own decisions about what he does. He likes to be free and not depend on others.
	q2112	Es ist ihm sehr wichtig, den Menschen um ihn herum zu helfen. Er will für deren Wohl sorgen.	It's very important to him to help the people around him. He wants to care for their well-being.
	q2113	Es ist ihm wichtig, sehr erfolgreich zu sein. Er hofft, dass die Leute seine Leistungen anerkennen.	Being very successful is important to him. He hopes people will recognise his achievements.
	q2114	Es ist ihm wichtig, dass der Staat seine persönliche Sicherheit vor allen Bedrohungen gewährleistet. Er will einen starken Staat, der seine Bürger verteidigt.	It is important to him that the government ensures his safety against all threats. He wants the state to be strong so it can defend its citizens.
	q2115	Er sucht das Abenteuer und geht gerne Risiken ein. Er will ein aufregendes Leben haben.	He looks for adventures and likes to take risks. He wants to have an exciting life.
	q2116	Es ist ihm wichtig, sich jederzeit korrekt zu verhalten. Er vermeidet es, Dinge zu tun, die andere Leute für falsch halten könnten.	It is important to him always to behave properly. He wants to avoid doing anything people would say is wrong.
	q2117	Es ist ihm wichtig, dass andere ihn respektieren. Er will, dass die Leute tun, was er sagt.	It is important to him to get respect from others. He wants people to do what he says.
	q2118	Es ist ihm wichtig, seinen Freunden gegenüber loyal zu sein. Er will sich für Menschen einsetzen, die ihm nahe stehen.	It is important to him to be loyal to his friends. He wants to devote himself to people close to him.
	q2119	Er ist fest davon überzeugt, dass die Menschen sich um die Natur kümmern sollten. Umweltschutz ist ihm wichtig.	He strongly believes that people should care for nature. Looking after the environment is important to him.

	q2120	Tradition ist ihm wichtig. Er versucht, sich an die Sitten und Gebräuche zu halten, die ihm von seiner Religion oder seiner Familie überliefert wurden.	Tradition is important to him. He tries to follow the customs handed down by his religion or his family.
	q2121	Er lässt keine Gelegenheit aus, Spaß zu haben. Es ist ihm wichtig, Dinge zu tun, die ihm Vergnügen bereiten.	He seeks every chance he can to have fun. It is important to him to do things that give him pleasure.

Demographics

School education		Die folgenden Fragen helfen, die Ergebnisse dieser Umfrage besser zu untersuchen. Hierfür benötigen wir auch einige Angaben zu Ihrer Person, die selbstverständlich anonym und vertraulich ausgewertet werden.	The following questions will help to better analyse the results of the survey. To this end, we also need some personal details that will, of course, be handled confidentially and evaluated anonymously.
	q22	Welchen höchsten allgemeinbildenden Schulabschluss haben Sie?	What is your highest level of general education completed?
		Noch Schüler	Still pupil or student
		Schule beendet ohne Abschluss	Left school without school-leaving certificate
		Hauptschulabschluss bzw. Volksschulabschluss	Hauptschule or Volksschule leaving certificate (compulsory basic secondary schooling)
		Abschluss der Polytechnischen Oberschule der DDR mit 8. oder 9. Klasse	Polytechnische Oberschule of the German Democratic Republic with a leaving certificate from Grade 8 or Grade 9
		Realschulabschluss (Mittlere Reife)	Realschule leaving certificate ("Mittlere Reife") (school-leaving certificate usually taken after the fifth year of secondary school)
		Abschluss der Polytechnischen Oberschule der DDR, 10. Klasse	Polytechnische Oberschule of the German Democratic Republic with leaving certificate from Grade 10
		Fachhochschulreife, den Abschluss einer Fachoberschule	Fachhochschulreife, leaving certificate from a Fachoberschule (technical secondary school)
		Abitur, allgemeine oder fachgebundene Hochschulreife bzw. Erweiterte Oberschule mit Abschluss 12. Klasse	General or subject-specific higher education entrance qualification (Abitur) from grammer school (Gymnasium) or extended secondary school (Erweiterte Oberschule, EOS) with leaving certificate from Grade 12, also EOS with apprenticeship; including Abitur from second-chance education
		einen anderen Schulabschluss, und zwar: ...	Other school-leaving certificate, namely: ...
Vocational education	q23	Welchen höchsten beruflichen Ausbildungsabschluss haben Sie?	What is your highest vocational qualification?
		noch in beruflicher Ausbildung	Still undergoing vocational education and training, including pre-vocational training year (Berufsvorbereitungsjahr), apprentice or trainee, intern, student
		ohne beruflichen Abschluss und auch nicht in beruflicher Ausbildung	No vocational qualification and not undergoing vocational education and training
		Lehre abgeschlossen	Apprenticeship completed
		beruflich-schulische Ausbildung abgeschlossen	School-based vocational education and training (Berufsfachschule, Handelsschule), inclusing preparatory service for the intermediate service in public administration, successfully completed
		Ausbildung an einer Fachschule der DDR abgeschlossen	Vocational education and training at a technical school (Fachschule) in the German Democratic Republic successfully completed
		Ausbildung an einer Fach-, Meister-, Technikerschule, Berufs- oder Fachakademie abgeschlossen	Vocational education at specialised academies and colleges of advanced vocational studies (Fachschule, Meisterschule, Technikerschule, Berufsakademie, Fachakademie) successfully completed
		Bachelor an einer (Fach-)Hochschule abgeschlossen	Bachelor's degree at a university or university of applied sciences (Fachhochschule) completed

		Fachhochschulabschluss (z. B. Diplom, Master)	Degree from university of applied science ("Fachhochschule) (e.g. Diplom, Master)
		Universitätsabschluss (z. B. Diplom, Magister, Staatsexamen, Master)	University degree (e.g. Diplom, Magister, Staatsexamen, Master)
		Promotion	Doctorate
		einen anderen beruflichen Abschluss, und zwar:	Another vocational qualification, namely
Household net income	q24	Wie hoch ist ungefähr Ihr monatliches Haushaltsnettoeinkommen? Ich meine dabei die Summe aus allen Einkommensquellen, die für Ihren gesamten Haushalt nach Abzug der Steuern und Sozialversicherungsbeiträge übrigbleibt.	About how high is your monthly net household income (the sum of all income sources that is available for the whole household after tax and social security contributions)?
		Unter 1000 Euro	Below 1,000 Euro
		1000 bis unter 2000 Euro	1,000 to 2,000 Euro
		2000 bis unter 3000 Euro	2,000 to 3,000 Euro
		3000 bis unter 4000 Euro	3,000 to 4,000 Euro
		4000 Euro oder mehr	4,000 Euro and more

What are people's attitudes towards big data? To answer this question, a nationwide survey of the German population (N = 1,331) was conducted to explore the attitudes towards different scenarios of big data practices that may have a direct impact on the personal self-development and lifestyle. The scenarios contained price discrimination in retail, credit scoring, differentiations in health insurance and in employment, and were described by some of the characteristics of big data practices, such as the use of internet data (e.g., from online social networking sites), automated decision-making by computers, and the selling of data to other companies. The study also addresses behavioural adaptations as possible reactions to big data practices and required protection measures. The attitudes towards the scenarios are examined in relation to demographic characteristics, personal value orientations, knowledge about computers and the internet, and general attitudes about privacy and data protection. Another focus of the study is on the institutional framework of privacy and data protection that realizes the fundamental principle of informational self-determination. The survey has revealed several challenges of big data practices for different elements of the current institutional framework, such as the informed consent approach with privacy policies, for the principle of purpose limitation, and the individuals' rights to request information about the processing of personal data and to have their data corrected or erased.

ISBN 978-3-7315-0859-5

9 783731 508595 >

ISSN 1869-9669
ISBN 978-3-7315-0859-5

Gedruckt auf FSC-zertifiziertem Papier