International Journal of Communication 13(2019), 1764–1783 1932–8036/20190005

Risk Perception and Privacy Regulation Preferences From a Cross-Cultural Perspective. A Qualitative Study Among German and U.S. Smartphone Users

LEYLA DOGRUEL
Johannes Gutenberg University Mainz, Germany

SVEN JÖCKEL
University of Erfurt, Germany

Following the notion that both individual privacy attitudes and (national) privacy regulation need to be addressed when understanding the privacy governance system, this article focuses on the relationship between information privacy risk perceptions and regulation preferences in two regulatory systems: Germany and the United States. Empirically, the study relies on semistructured interviews with German and U.S. smartphone users (*N* = 55). We analyze privacy risk perceptions and perceived control over privacy (RQ1), carving out four domains of privacy risks (governmental, criminal, and commercial misuse, as well as social risks). Furthermore, we focus on preferences for privacy regulation (RQ2), investigating preference for do-it-yourself privacy, as well as state- and market-based regulation. Findings support the notion that while privacy risks are shared among German and U.S. participants, U.S. users feel more in control over their data. A discrepancy between German and U.S. users with respect to their preferences for state- versus market-based regulation also exists.

Keywords: online privacy, privacy regulation, privacy risks, privacy preferences comparative research

With the rapid diffusion of online technologies on computers and more recently on mobile devices, the protection of personal information and behavior-related data has developed into a major topic in today's networked society (Acquisti, Brandimarte, & Loewenstein, 2015). Initially, research investigated online privacy, particularly in its relationship between social media use and self-disclosure (Trepte et al., 2017). Recently, however, the use of mobile technology has added another dimension of potential privacy threat when user behavioral data such as location-based data as well as body-function information (heart rate, calorie intake, etc.) are collected. Online privacy as such now also encompasses this notion of mobile privacy, further challenging individuals' ability to govern what information to disclose in their interactions (Ketelaar & van Balen, 2018).

Leyla Dogruel: dogruel@uni-mainz.de
Sven Joeckel: sven.joeckel@uni-erfurt.de
Date submitted: 2018–06–06

Previous research (Masur & Scharkow, 2016; Millham & Atkin, 2018) indicates that individual factors such as demographic variables, online experiences, and privacy literacy are related to individuals' (information) privacy attitudes and behaviors (Baruh, Secinti, & Cemalcilar, 2017). Less attention has been dedicated to the impact of contextual factors such as cultural orientations (Cho, Rivera-Sanchez, & Lim, 2009) and (national) privacy regulations (Bennett, Regan, & Bayley, 2017; Bellman, Johnson, Kobrin, & Lohse, 2004). In particular, existing research has either focused on examining privacy attitudes on an individual level (e.g., studying privacy attitudes and preferences in different countries; Trepte et al., 2017), or put the focus on the macro level by comparing national privacy regulation approaches (e.g., Baumer, Earp, & Poindexter, 2004). More recent studies point to the interrelation between individual privacy attitudes and (national) privacy regulation and call for a combination of both levels of analysis (Ginosar & Ariel, 2017; Lwin, Wirtz, & Williams, 2007; Miltgen & Smith, 2015).

Against this background, our study aims to investigate individual privacy risk perceptions and their relation with regulation preferences in the cases of German and U.S. smartphone users. We rely on a qualitative approach to determine what types of privacy risks users perceive and how far users differ in their preferences for privacy regulation systems.

Privacy on Individual and Societal Levels

Privacy Concerns and Perceived Risks

Privacy research relates to a broad range of disciplines (Smith, Dinev, & Xu, 2011) from law (Westin, 1967) to (social) psychology (Schwartz, 1968) and communication (Petronio, 2002). (Information) Privacy can be defined as an individual's control over what others know about him or her and involves four essential functions: (a) personal autonomy, (b) emotional release, (c) self-evaluation, and (d) limited communication (Westin, 1967). Privacy ranges on a continuum from too much (social isolation) to too little. It is a constant trade-off as to what others (friends, family, state, companies) should or should not know. Schwartz (1968) outlines that with respect to rules governing our protection of privacy, we have to distinguish between two levels: On the horizontal level, privacy intrusion may occur among individuals on the same level—our friends, peers, or family. On the vertical level, privacy is threatened by organizations and institutions such as private companies and state surveillance. Approaches to privacy management, such as Petronio's (2002) Communication Privacy Management Theory, often focus on the horizontal level but can also be transferred to the vertical level, whereas approaches on (national) privacy regulation mainly focus on the vertical level.

To protect their autonomy and privacy, users can employ a broad range of strategies to prevent either vertical or horizontal intrusions (Masur, 2019). Yet users often feel they have limited control of how they are able to regulate their privacy. Qualitative studies by Hargittai and Marwick (2016; in the U.S. context) and Hoffmann, Lutz, and Ranzini (2016; in the German context) report that individuals feel they have lost control over their information when using digital devices and even express resignation or cynicism about privacy violations and their inability to address the situation. Such cynicism occurs when users aspire to weight privacy risks and chances but are not able to fully grasp the complexity of the associated risks,

leading even to what Choi, Park, and Jung (2018) recently described as privacy fatigue—a psychological effect of no longer being able and willing to protect one's privacy.

The findings in such studies share the assumption of an attitude-behavior gap between privacy attitudes and privacy behaviors insofar as people are concerned about privacy but do not behave accordingly in the digital environment (also labelled a privacy paradox)—or are not able to behave so (Choi et al., 2018). In recent years, several empirical studies (for an overview see Kokolakis, 2017; Barth & de Jong, 2017) have addressed this phenomenon. However, results are disparate, often indicating significant yet weak effects in either direction, as underlined by Baruh et al. (2017) in their meta-analytic review. These systematic reviews indicate that the existence of a privacy paradox is likely to be a function of the concrete theoretical perspective, for instance, privacy calculus (Chen, 2018) or a heuristics-and-biases approach (Acquisti et al., 2015; for an overview of different theoretical perspectives, see Barth & de Jong, 2017) or the media (social networking service [SNS], apps, etc.) in the focus of research. Giving one example, Dienlin and Trepte (2015) demonstrate that these theoretical and hence methodological implications can lead to different outcomes. Based on the Theory of Planned Behavior, they show that privacy attitudes, which are broader in scope and bipolar, can influence privacy intentions, which are an antecedent to privacy behaviors. Yet the direct link from privacy concerns, which are narrower and unipolar (negative), to privacy intentions argued for in other studies was not found. Nevertheless, privacy concerns had an indirect effect on privacy intentions mediated through privacy attitudes. Zhou and Li (2014) further underline the assumption of indirect effects with respect to privacy outcomes (behaviors/intention). They sum up their research by claiming that privacy concerns affect privacy risks, which then affect usage. With respect to mobile media, a recent study by Ketelaar and van Balen (2018) demonstrates that privacy concerns have a positive effect on privacy behaviors such as the adjustment of privacy settings on smartphones. Further, in examining digital skill disparities, studies indicate that age and gender, as well as income and (lack of) social resources, not only affect the use of the Internet in general but also privacy in particular (e.g., Park 2015; Madden, Gilman, Levy, & Marwick, 2017).

Overall, we argue that privacy intrusion can occur both between users and other users and between the user and the state, or commercial actors. Perceived privacy risks as such may account for both these levels and are likely to influence people's actual privacy behavior. Yet we still know little about the relationship between a particular cultural context and media users' perceptions of privacy risks.

Privacy From a Cross-Cultural Perspective

The notion that privacy is a culture-dependent concept is not at all new (Farrall, 2008). Referring to ethnographic studies, Altman (1977) argues that privacy is a universal phenomenon, and he points out that members of all cultures have developed some kinds of mechanisms to regulate their privacy. However, these mechanisms vary and reveal considerable differences in what is considered as private in different contexts. According to Communication Privacy Management Theory, culture is among the "core" criteria influencing the formation of privacy rules (Petronio, 2002). Individuals are socialized into certain norms for privacy depending on their cultural background. With culture representing a core resource for individuals to develop rules that guide their behaviors, privacy values determine how people manage their privacy (Baruh et al., 2017; Petronio, 2002).

Empirically, research supports the notion of cross-cultural differences in privacy attitudes and preferences. In the case of social networks, studies indicate cultural differences in the use of SNS with respect to the disclosure of private information such as sharing photos or using pseudonyms (Ur & Wang, 2013). Results, for instance, show stricter privacy boundary management by users from collectivistic cultures such as China (Liang, Shen, & Fu, 2016). A study of German, Dutch, British, U.S., and Chinese social media users indicates that individuals from countries who rank high in uncertainty avoidance (Germany, Netherlands) perceive greater privacy risks than those from individualist countries (UK, U.S.; Trepte et al., 2017). Older, large-scale studies on a diverse set of countries examine how cultural values (e.g., individualistic vs. collectivistic orientations) and different types of national privacy regulation affect individuals' privacy perceptions (Bellman et al., 2004; Cho et al., 2009; Milberg, Smith, & Burke, 2000). Comparing regulatory approaches to privacy between Europe and the United States, Movius and Krup (2009), for instance, show that differences in culture-specific privacy values and social norms affect national privacy policy.

Privacy Regulation as a Governance System

A growing body of research argues for an integration of individual-level approaches to privacy, focusing on privacy attitudes, concerns, and risk perception with regulatory approaches that investigate governance structures and apply a legal perspective (Ginosar & Ariel, 2017; Martin & Murphy, 2017; Miltgen & Smith, 2015; Smith et al., 2011). These approaches aim at connecting users' privacy attitudes and behaviors with research on the ethical and legal responsibilities of information privacy regulation (e.g., Lwin et al., 2007). This results in a multilayered privacy governance system in which a country's regulatory structure and its citizens' privacy behavior are intertwined through an indirect feedback process (Milberg et al., 2000). In democratic societies, citizens support and vote for parties and politicians but also interest groups that advocate different regulatory approaches, and so a country's regulation approach (ideally) reflects the desires of its citizens. By this logic, culture is an antecedent of a nation's regulation of information privacy (Cockcroft & Rekker, 2016). Individuals who perceive that legal regulations in their country are weak are more likely to perceive a risk that their information is being used inappropriately (Lwin et al., 2007), and individuals with high privacy concerns are more likely to call for additional legal interventions (Milberg et al., 2000) or support the political parties and interest groups that advocate their interests (Löblich & Wendelin, 2012). When Internet users do not perceive the current scheme of self-regulation as adequate, they prefer stronger (state) intervention, which can eventually lead to a regulatory response (Smith et al., 2011). Yet such feedback loops are only likely if users are sufficiently aware and empowered to demand such responses. Furthermore, research has also pointed to a negative effect insofar as when users have strong trust in the government's regulatory system, they feel they can behave in a less cautious way in their online interactions (Miltgen & Smith, 2015). Even if privacy regulation often occurs on the transnational level, as for instance with the European General Data Protection Regulation (EU, 2018), cultural differences still lead to different implementations of privacy regulations, as Custers, Dechesne, Sears, Tani, and van der Hof (2018) outline for EU member states.

Consequently, and arguing from a societal perspective, the regulation of online privacy can be characterized as a complex web of different actors, levels (national, transnational), and regulatory approaches that involves multiple stakeholders including businesses, government agencies, and civil society (Flyverbom, Deibert, & Matten, 2017; Newman, 2014). Because of shifting alliances among government, industry groups,

and users, privacy regulation is depicted as a multistakeholder governance structure (Marsden, 2008). Within this structure, two main approaches are prevalent on how to protect privacy (Hirsch, 2011): government regulation that aims at restricting companies' data collection and processing procedures as well as market or industry self-regulation.

Most (national) approaches toward privacy regulation integrate legal instruments, such as laws addressing the handling of personal information, with self- and co-regulatory approaches that rely on codes of practice as well as norms and rules (Busch 2010; Hirsch, 2011). Within the privacy governance system, users also play a crucial role in the protection of information privacy. Matzner, Masur, Ochs, and von Pape (2016) introduced the term "do-it-yourself" (DIY) privacy to describe data protection measures on the level of individual consumers. In fact, users report a broad range of privacy prevention measures such as the use of fake names on online platforms and the adjustment of privacy settings or visibility on SNS (Matzner et al., 2016). These forms of self-help in privacy protection are considered an adequate measure against privacy risks in particular in market economies—even though these measures are again subject to digital skill disparities (Büchi, Just, & Latzer, 2017).

Privacy Risks and Regulation Preference in Germany and the United States

We see individuals' privacy behavior as a consequence of their privacy attitudes and more concretely as a consequence of privacy risks perceptions. These factors have been extensively studied on the individual level (Dienlin & Trepte, 2015; Miltgen & Smith, 2015). We also argue that individuals are not isolated in their privacy behavior, but rather embedded in a wider cultural system. Within this system, certain privacy regulation systems prevail. Mainly, we focus on three potential methods for privacy regulation: state intervention, a more market-based self-regulatory approach, and DIY privacy on the part of users.

The three approaches are not mutually exclusive, and depending on the cultural context, we expect to find differences in users' perceptions of the division of responsibility among different actors. We also expect those differences to be prevalent in Western, industrialized countries as similar as the United States and Germany. As suggested by a study by Bennett et al. (2017), crucial differences in privacy (or consumer) regulation even exist between countries as close as the United States and Canada, with the latter's regulation system resembling the European privacy regulatory approach of seeing privacy as a (constitutional) right. Loosely following a most similar case design (Przeworski & Teune, 1970), where two cases for comparison share most characteristics but differ in the variable of interest, and being familiar with the United States and Germany, our empirical focus is on these two countries.

U.S. and German citizens share concerns about privacy. According to the Pew Research Center, in 2014/2015, 52% of Americans reported to be at least somewhat concerned about the government surveilling their data and digital communication. A majority of 57% found it unacceptable for the government to monitor the communication of U.S. citizens (Rainie, 2016). A representative survey among EU citizens found that 70% of Germans are concerned about potential misuse of their data. Also, Germans rank highest with respect to the proportion of citizens having heard about mass data collections (European Commission, 2015). One of the few cross-country comparisons on privacy attitudes highlights several differences as well: Trepte and Masur

(2016) show that Germans were more active in privacy management, applied more privacy settings, and were more likely to restrict the visibility of profile info than U.S. participants.

Comparing German and U.S. Facebook users, Krasnova, Veltri, and Günther (2012) demonstrated that U.S. users have a higher trust in the service provider (Facebook) to safeguard their privacy and feel more in control over their personal data than Germans. These differences translate into a higher disclosure of information among U.S. users—a result supported by findings by Karl, Peluchette, and Schlaegel (2010) indicating that U.S. users are more likely to post confidential information to their Facebook site than Germans.

Differences between the United States and Germany become more obvious when we focus on the privacy governance system. From a legal perspective, studies comparing European privacy regulations (including Germany) with the U.S. system point to fundamental differences (Hirsch, 2011; Movius & Krup, 2009). In the European tradition, privacy is considered a fundamental human right that is a precondition for individuals' autonomy and freedom and cannot be traded away. In this value-based approach, privacy is seen as a right guaranteed by the legal system. In contrast, the United States is more likely to perceive privacy as a commodity that can be subject to (economic) exchanges and cost-benefit calculations between the interests of individuals and society (Walsh, Parisi, & Passerini, 2017). As a result, the legal system treats privacy like property, granting Internet users privacy property rights (Busch, 2010). These different approaches to privacy are related to a stricter governmental omnibus privacy regulation under the umbrella of EU data protection with the recently updated General Data Protection Regulation (GDPR). Germany, in particular, is as an early example of establishing legal privacy protection policies (Ginosar & Ariel, 2017). The United States, in contrast, has adopted a more liberal approach to privacy regulation by developing a narrowly targeted solution based on a sectoral approach and self-regulation based on industry standards (Baumer et al., 2004; Movius & Krup, 2009).

We set out to describe the interrelationship between individual-level privacy attitudes (particularly privacy risk perceptions) and regulatory preferences within two different regulatory systems in two Western cultures, Germany and the United States. We do so by focusing on smartphone users to account for elements of privacy that encompass privacy behaviors such as self-disclosure but also concepts that focus on behavioral data that can be shared with mobile devices. For the concrete empirical analysis, we adopt a rather open and exploratory approach by interviewing German and U.S. smartphone users about their perceptions of privacy risks and their privacy regulation preferences. First, we ask what German and U.S. smartphone users perceive as privacy risks and how far they feel in control over their data (RQ1). Second, we investigate preferences for privacy regulation (RQ2). Here we ask users whom they see as responsible and whom they trust. We do so by focusing on the three potential regulatory perspectives: state focused, market based, and DIY privacy.

RQ1: What are German and U.S. smartphone users' perceptions of privacy risks, and how far do they feel in control of their data?

RQ2: What are German and U.S. smartphone users' preferences for privacy regulation: state focused, market based, or DIY privacy?

Method

Data Collection and Participants

Given the exploratory nature of our research design, we relied on a qualitative approach using semistructured interviews to determine German and U.S. smartphone users' privacy risk perceptions and regulation preferences. All participants had to qualify for the study by using at least one mobile device such as a smartphone. Interviews were conducted by two trained interviewers in Germany and by the research team in the United States. German participants were recruited following a guideline to focus on working adults. For the United States, recruitment took place through a mailing list of faculty and staff at a U.S. university. Both samples were complemented by recruiting four to five student participants. In total, we carried out 55 interviews (U.S.: 28, Germany: 27). Participants' mean age was around 30 years in Germany and slightly older (38 years) in the United States. Women were overrepresented in the United States (69%) compared with the German sample (44%). While such a sample is by no means representative for German or U.S. smartphone users, it allows for some variance with respect to sociodemographics. The goal of our sampling process was to account for a diverse set of participants and a broad range of opinions.

We employed the same, translated interview guideline for the German and U.S. interviews. Interviews lasted around one hour and ranged from 45 to 80 minutes. After permission was granted, the interview was recorded and later transcribed. The interviews started with some open questions on participants' digital media use (devices, applications) and then moved to their perception of privacy. The focus of our research is on the question of privacy risks and regulation preferences.

Privacy risk perception was addressed with several open-ended questions such as *In your opinion, what are possible risks that are associated with the revelation of personal information?* or targeting threats of surveillance: *Are you concerned about "authorities" misusing personal data?* Related to the perception of privacy risks, and as a further step, we asked how much the participants themselves feel in control of what happens with their personal data, and finally, we investigated their preference for privacy regulation strategies.

Analysis

We employed a combination of an emerging coding scheme as well as a theory-driven approach for qualitative content analysis. The emerging coding scheme was used for privacy risk perceptions. This required multiple readings of the material, after which one coder generated a code for each new potential risk mentioned by our participants (Mayring, 2000). Each risk was then either added into one of these existing categories or generated a new category. In a second step, these emerging codes where condensed into superordinate risk categories. For each category, participants' arguments were grouped and illustrative quotes singled out (Hargittai & Marwick, 2016). Based on this deduction of categories, a comprehensive interpretation was written. This interpretive text was then condensed for the presentation of results.

For the analysis of privacy regulation preferences, we employed a theory-driven approach and developed three distinct categories based on our theoretical assessment of regulatory practices: (a)

preference for market-based regulation, (b) preference for state-based regulation, and (c) elements of DIY privacy (regulation). Participants' statements were then grouped into these three major categories. All coding procedures were carried out with the MAXQDA software package for qualitative data analysis. For the presentation of results, we present illustrative quotes as direct citations from our material, but we also rely on indirect references, in which we present a selection of participants making similar claims.

Results

Privacy Risk Perception (RQ1)

Across all interviews, we see four central areas of privacy risks: data misuse by authorities, by criminals, and by commercial actors, as well as social privacy risks. Most important, these four risk categories are not independent from each other, and some perceived risks run across all four domains (or at least two or three). For analytical purposes, we separated our analysis of these four risk categories.

Misuse of Data by Authorities

A common theme is the misuse of data by authorities, namely law enforcement or the state in general. This risk is clearly positioned on the vertical privacy level. Overall, concerns for misuse of data by authorities ranged from "very much" (U16, female, 34)[1] to "not at all" (U17, female, 34). Risks were "vague" (G4, female, 20) or "latent" (G3, female, 49). Most participants were rather unconcerned about themselves or their families becoming victims of data misuse by authorities as they "do not intend to become an enemy of the state" (G19, male, 22[Q1]) or they are "a white, male around middle-class" (U20, male, 25) person and hardly of interest to intelligence services. Participants also stated this may only be true because they live in the United States or Germany. Living in the former German Democratic Republic (GDR) or during Nazi Germany, but also in countries such as China or Russia, could mean substantially higher risk of surveillance (G5, U6). Interestingly, two German participants also saw the United States as a state where the risk of surveillance is considerably higher than in Germany (G14, G17).

With some notable exceptions, participants in both countries (e.g., U26, U25, G3, G11) saw the risks of data misuse by authorities as higher for individuals connected to extremist groups, such as Islamist groups including ISIS (e.g., U9, G16) or even Muslims in general (U17, G17), but also, from a German perspective, those from the far right (e.g., G9, G18). Overall, participants believed the scrutiny of those groups to be positive and saw it as a means to protect the constitution (e.g., U9, G19, G22), but we also heard some critical voices: U8 (female, 35) was "sure" there are algorithms that focus on certain groups, and "I am sure they are totally racist." Refugees and those assisting refugees are one group perceived as being unjustifiably under scrutiny (U5, G23).

[1] Participants in direct quotes are indicated by U = U.S., G = German, a running number, and the participant's gender and age. Participants in direct quotes are indicated only by country and running number. For the German quotes, we also added a running number of the quote (e.g., Q1–Q6) to reference the original German quote in the appendix.

The misuse of data by authorities was directly related to the question of whether collecting more data increases national security. We saw a rather diverse picture here. Some participants (e.g., G11, G22, U17, U23) argue that data collection "definitely" (G5, male, 55) increases national security. Others clearly oppose this perception (e.g., G12, G16, U1, U11). A third, and potentially the largest, group saw the question as "a double-edged sword" (U16, female, 34) balancing freedom and safety (U10). Participants either saw that effort and effect are not in balance (G13, G14), stated that increases in security through data collection work only "to a small extent" (G9, male, 25), or only in certain, limited areas (U6, G17).

Criminal Misuse

The risk of the use of personal data for criminal purposes is a broad category and encompasses risks of fraudulent financial transactions, identity theft, and computer viruses. With respect to horizontal and vertical levels of privacy, this risk category largely focuses on risks on the vertical level concerning the relationship between users and enterprises and potential infringements through criminal actors. However, risks on the horizontal level, when personal information may be misused for identity theft, also become apparent.

The risks of data misuse for financial transactions, namely phishing or credit card misuse, were central for both U.S. and German participants. Risks mentioned by participants included hacking of (online) banking accounts (e.g., G18, G22, U14, U15) and misuse of credit card information in conjunction with identity theft (U1, U26). The severity of the risks was judged strikingly differently by individual participants. Some saw online banking in general as "super dangerous" (G4, female, 20[Q2]; also U22); others had complete trust in the abilities of banks to secure their (mobile) services (G17, U5).

Across U.S. and German participants, the sharing of one's location was seen as the biggest privacy risk as it could allow criminals to either assault (G1, G21, U12) or kidnap a person (G18), but most likely, burglaries while away are seen as the most likely risk (G2, G11, U13). Personal data may be hacked and become available online (e.g., U4, G3, U17). G16 (male, 31[Q3]) connected the risk of misuse by criminals with the misuse by commercial actors; while the first is less likely but troublesome, the latter is something "you cannot do anything against."

Misuse by Commercial Actors

Compared with the risk of misuse by authorities or by criminals, the risk of misuse by commercial actors clearly trailed in terms of importance in both countries. Again, the focus here is much more on the vertical level of privacy. Participants in both countries saw the problem of tracking user behavior for marketing purposes as the biggest risk (for instance G12, G20, U10, U20). The existing possibilities for targeting users were seen as "creepy" (U16, female, 34) or even "insane" (U5, female, 28). A few participants mentioned risks with respect to location tracking but had gotten used to using such services (U7, G13). U11 (male, 60), for instance, saw risks and opportunities as "a fair trade-off."

Social Privacy Risks

Social privacy risk is another broad category of perceived privacy risks that encompasses risks for personal privacy boundaries or communication practices—it closely resembles what Raynes-Goldie (2010) describes as social privacy. In contrast to the other three major risk categories, this category centers more around the horizontal level of privacy and therefore includes risks that may occur in the management of privacy on a personal level.

The most prominent concern is that others may know more about you than you as a user are willing to give away. Germans tended to mention this risk more often than U.S. participants. German users feared becoming "a Man of Glass" (G22, male, 30[Q4])—a "gläserner Mensch," a typical German expression for describing that others may see your deepest inside. Others in this respect can be other users (G12), commercial actors (G17), or one's employer (G21, G23), a risk shared by U.S. participants as well (U4, U23). Critical issues among German participants related to personality (G12, G22) but also location and movements (G17, G25). Related to this was the risk of losing control of who has access to your personal data (G12, U21, U17) such as your contact lists. When looking into these social privacy risks, Germans are more likely to mention risks that relate to the social level than U.S. participants.

Perceived Control Over Privacy Protection

In contrast to perceived privacy risks, we see substantial differences between German and U.S. participants in terms of perceived control over privacy protection. With few exceptions, German participants believe they have little control of what happens with their data. One common emerging theme was that people only have control of their personal data as long as they do not post online (e.g., G11, G3). Personal control thus centers on the question of what you post online and which services you use. After this decision has been made, users were seen to have given away any control over their own data.

Some U.S. and German participants described their level of control as medium—some things they can control, other are beyond their scope and ability (e.g., G15, G26, U1, U3). Yet a stronger feeling of control over their own data was prevalent among U.S. participants (e.g., U23, U24): "I hope I have a lot of control" (U11, male, 60). Only a few U.S. participants saw a lack of control over their personal data (e.g., U27, U9).

In summary, U.S. participants saw themselves as more in control of their personal data than Germans—although the privacy risks both groups saw were rather similar.

Privacy Regulation Preferences (RQ2)

Responsibility of Privacy Regulation

Participants mostly believe the responsibility for the protection of privacy lies primarily in their own hands (i.e., U9, U7, G4, G29). G18 (male, 19[Q5]) clearly states: "Of course it's me who is responsible for using password protection and stuff like that. That would be like, if I do not lock my house and someone

breaks in, then it would be my fault." Both German as well as U.S. participants thus seem to favor DIY privacy, seeing themselves as responsible for applying privacy management measures. At the same time, participants also stressed that using these services was not entirely their personal decision because of the social pressure associated with opting out from communication platforms such as Facebook.

Our findings were mixed on the responsibility of corporate and state actors—a result reported in previous research as well (Hargittai & Marwick, 2016). Some participants argued that the government is primarily responsible for protecting users' privacy online, in particular by providing the legal framework for privacy protection (e.g., G1, G13). Also, some German participants mentioned concrete governmental institutions or actors responsible for the regulation of privacy such as consumer protection law (G16) or privacy data protection officers (G17) or the EU as a transnational governmental body (G12). However, despite the possible effectiveness of governmental privacy protection, participants also pointed to its limits. G14 (female, 24[Q6]), for instance, identified a failure of the government with regard to effective privacy protection:

> Actually, I feel that the government should be responsible to protect our privacy. However, I don't think that they do enough. This is why I have to "catch up" myself, so to say. But not because I want to, but because I feel it's inadequate.

This perception of the government as primarily responsible for privacy protection also supports our expectation that German users are more likely to call for state intervention in the case of privacy: All but one (U18) of our participants who ranked the government's responsibility first were German.

Only a few U.S. and not a single German interviewee saw commercial actors such as hardware manufacturers or service providers as primarily responsible for privacy protection (e.g., U12, U25). This is again in support of the notion that in the United States, individuals are more likely to see the industry itself as responsible for protecting their clients' private information. One U.S. participant, for instance, explained how mobile phone manufacturers could implement their responsibility by educating users after purchasing a device (U8). However, even though most participants did not consider government or private actors to hold the greatest responsibility for privacy, they still believed both carry some responsibility, or as one participant put it: "I'd like to say it's a nice balance between myself, the companies, and then also the government. I would like to see it be a three-way thing" (U20, male, 25). The government in particular needs to set "minimum standards" of privacy protection comparable to safety standards for the use of cars (U13, male, 55).

Attribution of Trust in Privacy Regulation

Our participants consistently expressed that they had the highest trust in themselves as well as their closest friends and family to protect their private information in digital contexts. The state as well as commercial actors were perceived as less trustworthy. According to one interview (U3, female, 43): "She: I think in an ideal world I would trust the government. Interviewer: And in a not-so-ideal world? Probably in the real world? She: Myself."

We saw diverging views on the question of whether to trust governmental and state actors or commercial actors to protect privacy. We found German participants were more likely to express that they trusted the government than U.S. participants. In the case of commercial actors, participants in both countries mentioned some kind of "conditional" trust insofar as they only trust particular actors such as their bank (G23; U11), smaller online shops (G14, G17) and, in the case of Germany, German-based e-mail services (G24). Even though U.S. participants also expressed some distrust in private actors, they are more likely to refer to "big brands" they trust such as phone manufacturers (Apple, Samsung) or online services (Amazon, Google, PayPal; e.g., U19, U24).

Preferences in Privacy Regulation

Even though our participants seem to have some shared opinions about their personal role in protecting their privacy, we also witnessed crucial differences that particularly relate to the role of the state (governmental) and private actors (industry regulation): While German participants consistently perceived that the government should provide a legal framework addressing the misuse of personal information by private actors, U.S. participants also felt the government itself should consider its limits on the collection and processing of citizen data for security purposes. One of our interviewees explicitly said:

> Not necessarily for protecting us, no. I think they [the government] have a responsibility to not make it easy for entities like the police or national security or central intelligence or whatever. They have a responsibility to make sure those entities are not misusing or gathering information that they don't have good reason to gather. (U3, female, 48)

On the responsibility of commercial actors, we observed disagreements among participants. Some strongly believed they are responsible for data protection (e.g., G10, G2, U13, U23) while others did not:

> Since the question of responsibility is in my view a moral one, no. This is about economic companies that think economically. If it were up to them, I should best send them the size of my underpants. That's why I do not see the companies as having responsibility. Simply because it is the wrong approach to consider them as moral institutions. (G19, male, 22[Q7]; similar: G13, G21, U14, U22)

In the United States, the controversy around Apple's refusal to grant the FBI access to an iPhone used by one of the San Bernardino shooters,[2] who killed 14 people in an act of terrorism, shows how critically the responsibility of commercial actors can be judged. As our participants argued, private corporations are seen as even protecting their customers' privacy against access by (state) authorities (U10, U12).

Taken together, DIY privacy is seen as the preferred regulation strategy. Balancing governmental and commercial actors as agents in the privacy governance systems, German participants at large tend to favor governmental regulation whereas U.S. participants give more credit to commercial actors.

---

[2] For more information see Wikipedia, "FBI-Apple Encryption Dispute," https://en.wikipedia.org/wiki/FBI–Apple_encryption_dispute

Discussion

During the process of digitization, individuals' privacy has come under threat. The revelation of the U.S. government's involvement in massive surveillance activities in the context of the National Security Agency (NSA)/Snowden affair (re)activated the societal debate over privacy versus security approaches (Hosein, 2017; Reddick, Chatfield, & Jaramillo, 2015; Wahl-Jorgensen, Bennett, & Taylor, 2017). Most likely as a result of this, we can identify a more accentuated critical perspective on the government's surveillance program in the United States (in the "post-Snowden era"; Rainie & Maniam, 2016). More recently, the illegitimate collection of personal data by Cambridge Analytica (Confessore, 2018; Solon, 2018), and claims that these data were used in political campaigns from the Brexit Referendum to the 2016 U.S. presidential election, has not only led to Facebook's CEO, Mark Zuckerberg, testifying to the U.S. Congress and European Parliament, but may have further increased the notion that people's privacy is threatened. This time, it is not so much government surveillance, but the illegal or illegitimate use of personal data by commercial enterprises.

Within this context, our analysis outlined that the regulation of information privacy is a privacy governance system involving three core players: the state, commercial entities, and the user. Privacy then needs to be regulated both with respect to horizontal as well as vertical threats. To understand this interrelationship, we focused on smartphone users and their privacy attitudes and contextualized these with background factors such as cultural orientations about privacy and (national) privacy regulations.

When focusing on individuals' privacy risk perceptions, we found that both German and U.S. smartphone users mentioned a broad range of potential risks. These risks were very individual in nature, and being German or U.S. explains very few differences in the attribution of privacy risks. The only crosscultural difference we saw related to social risks, particularly risks related to the horizontal level of privacy, where Germans were more concerned than U.S. participants. However, there were starker cross-cultural differences in perceptions about users' control over their own data. Here, we found more confidence among U.S. users in terms of their ability to control their data, whereas German users predominantly held more skeptical views.

Despite perceiving rather similar privacy risks, German and U.S. users also differed with respect to their preferences for privacy regulation systems. While German participants articulated a stronger preference for state regulation, U.S. participants exhibited a higher trust in themselves (users) as well as commercial actors (manufacturers and service providers) to protect their data. We suspect that these differences in the preference for privacy regulation are related to differences in the perceived control over their own data between German and U.S. participants. Although U.S. as well as German individuals showed a preference for DIY privacy, Germans were much more skeptical about the extent of control they had over their own data in a digitized world. Consequently, we suspect they are more likely to demand governmental actions and more willing to accept state privacy regulations.

This opens the ground for a further debate on the multilayered notion of privacy governance. We may speculate that the differences between U.S. and German participants with respect to privacy regulation strategies in spite of similar privacy risk perceptions are a consequence of living in a particular regulatory

system. At the same time, however, we also argue for the reverse effect: Citizens' preferences for specific regulations may also lead to the implementation of distinct regulatory systems. At least in Western democratic societies, citizens can articulate their preferences through participating in the political process or political activism (Löblich & Wendelin, 2012). As a result, privacy governance can be depicted as a mutual and reciprocal relationship with regulatory systems not only shaping people's preferences but also being shaped by them.

Based on our findings, we recommend future research examining privacy behaviors and privacy governance to account for the multilayered dimensions in the context of privacy. While our study largely focused on the layer of privacy regulation as one contextual dimension, further aspects such as individuals' resources and competences, and digital disparities, need to be taken into account when examining differences in privacy governance systems. Also, more research is needed to examine the concrete relationship between individual privacy preferences, attitudes, and behaviors and the regulatory context and its development over time, as Bennett and Raab (2018) argue.

Still, we need to be cautious about making causal claims. In our research, we opted for a rather open and exploratory approach. On the one hand, this gave us the opportunity to identify both privacy risks as well as regulation preferences as identified by the participants themselves. On the other hand, this does not allow us to make any causal claims, and we can only speculate as to how these constructs are related and whether they are a function of cultural contexts.

We relied on two different samples, and both samples were far from representative of the U.S. or German population. In both cases, the samples were taken from academic contexts and were therefore highly educated, mostly employed, and experienced user groups of digital media. These groups were rather self-aware of current developments in information privacy and were able to elaborate on the issues. However, even though these participants cannot be seen as "average" German or U.S. citizens, they allowed a thorough investigation of privacy risks and regulation preferences of individuals living within two different regulatory systems.

Last, as Dienlin and Trepte (2015) argue, we need to be aware of the distinction between privacy attitudes and concerns. What our participants mentioned is closer to actual privacy concerns, and so we still know little about how these concrete concerns then shape overall privacy attitudes.

In this respect, our research has laid some groundwork for further investigations on the relationship among privacy attitudes, privacy regulation, and cultural context, not only with respect to the United States and Germany. Future research is recommended to continue our pursuit of integrating the cultural context and regulatory system into research that focuses on individuals' privacy attitudes. Such research, relying on broad, representative samples, may then also investigate testable models on the relationship among privacy attitudes, concerns, and risk perception and preferences for specific regulatory systems.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi:10.1126/science.aaa1465

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, *33*(3), 66–84.

Barth, S., & de Jong, M.D.T. (2017). The privacy paradox—Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi:10.1016/j.tele.2017.04.013

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53. https://doi:10.1111/jcom.12276

Baumer, D. L., Earp, J. B., & Poindexter, J. C. (2004). Internet privacy law: A comparison between the United States and the European Union. *Computers & Security*, *23*(5), 400–412. https://doi:10.1016/j.cose.2003.11.001

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, *20*(5), 313–324. https://doi:10.1080/01972240490507956

Bennett, C. J., & Raab, C. D. (2018). Revisiting the governance of privacy: Contemporary policy instruments in global perspective. *Regulation & Governance*, *1*(6), 142. https://doi:10.1111/rego.12222

Bennett, C., Regan, P., & Bayley, R. (2017). If these Canadians lived in the United States, how would they protect their privacy? *First Monday*, *22*(3). https://doi:10.5210/fm.v22i3.6817

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of Internet skills for online privacy protection. *Information, Communication & Society*, *20*(8), 1261–1278. https://doi:10.1080/1369118X.2016.1229001

Busch, A. (2010). The regulation of privacy*. Jerusalem Papers in Regulation & Governance* (Working Paper No. 26). Retrieved from http://regulation.huji.ac.il/papers/jp26.pdf

Chen, H.-T. (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American Behavioral Scientist*, *62*(10), 1392–1412. https://doi:10.1177/0002764218792691

Cho, H., Rivera-Sanchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society*, *11*(3), 395–416. https://doi:10.1177/1461444808101618

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi:10.1016/j.chb.2017.12.001

Cockcroft, S., & Rekker, S. (2016). The relationship between culture and information privacy policy. *Electronic Markets*, *26*(1), 55–72. https://doi:10.1007/s12525-015-0195-9

Confessore, N. (2018, April 4). Cambridge Analytica and Facebook: The scandal and the fallout so far. *New York Times.* Retrieved from https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, *34*(2), 234–243. https://doi:10.1016/j.clsr.2017.09.001

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297. https://doi:10.1002/ejsp.2049

EU (European Union). (2018). *2018 reform of EU data protection rules.* Retrieved from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

European Commission. (2015). *Special Eurobarometer 431: Data protection*. Retrieved from http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf

Farrall, K. N. (2008). Global privacy in flux: Illuminating privacy across cultures in China and the U.S. *International Journal of Communication*, *2*, 993–1030. Retrieved from http://ijoc.org/index.php/ijoc/article/view/370/228

Flyverbom, M., Deibert, R., & Matten, D. (2017). The governance of digital technology, big data, and the Internet: New roles and responsibilities for business. *Business & Society*, *114*(768). Advance online publication. https://doi:10.1177/0007650317727540

Ginosar, A., & Ariel, Y. (2017). An analytical framework for online privacy research: What is missing? *Information & Management*, *54*(7), 948–957. https://doi:10.1016/j.im.2017.02.004

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 3737–3757. Retrieved from http://ijoc.org/index.php/ijoc/article/view/4655/1738

Hirsch, D. D. (2011). The law and policy of online privacy: Regulation, self-regulation, or co-regulation? *Seattle University Law Review*, *34*(2), 439–480.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4). https://doi:10.5817/CP2016-4-7

Hosein, G. (2017). Digital citizenship and surveillance. Compromising over technology, security, and privacy—Commentary. *International Journal of Communication*, *11*, 902–906. Retrieved from http://ijoc.org/index.php/ijoc/article/view/6825/1938

Karl, K., Peluchette, J., & Schlaegel, C. (2010). Who's posting Facebook faux pas? A cross-cultural examination of personality differences. *International Journal of Selection and Assessment*, *18*(2), 174–186. https://doi:10.1111/j.1468-2389.2010.00499.x

Ketelaar, P. E., & van Balen, M. (2018). The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior*, *78*, 174–182. https://doi:10.1016/j.chb.2017.09.034

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi:10.1016/j.cose.2015.07.002

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering*, *4*(3), 127–135. https://doi:10.1007/s12599-012-0216-6

Liang, H., Shen, F., & Fu, K.-W. (2016). Privacy protection and self-disclosure across societies: A study of global Twitter users. *New Media & Society*, *19*(9), 1476–1497. https://doi:10.1177/1461444816642210

Löblich, M., & Wendelin, M. (2012). ICT policy activism on a national level: Ideas, resources and strategies of German civil society in governance processes. *New Media & Society*, *16*(6), 899–915. https://doi:10.1177/1461444811432427

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, *35*(4), 572–585. https://doi:10.1007/s11747-006-0003-3

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review*, *95*(1). Retrieved from http://openscholarship.wustl.edu/law_lawreview/vol95/iss1/6

Marsden, C. (2008). Beyond Europe: The Internet, regulation, and multistakeholder governance—Representing the consumer interest? *Journal of Consumer Policy*, *31*(1), 115–132. https://doi:10.1007/s10603-007-9056-z

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155. https://doi:10.1007/s11747-016-0495-4

Masur, P. K. (2019). *Situational privacy and self-disclosure: Communication processes in online environments*. Cham, Switzerland: Springer International.

Masur, P. K., & Scharkow, M. (2016). Disclosure management on social network sites: Individual privacy perceptions and user-directed privacy strategies. *Social Media + Society*, *2*(1). https://doi:10.1177/2056305116634368

Matzner, T., Masur, P. K., Ochs, C., & von Pape, T. (2016). Do-it-yourself data protection—Empowerment or burden? In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Data protection on the move: Current developments in ICT and privacy/data protection* (pp. 277–305). New York: Springer. https://doi:10.1007/978-94-017-7376-8_11

Mayring, P. (2000). Qualitative content analysis. *Forum: Qualitative Social Research*, *1*(2). Retrieved from http://nbn-resolving.de/urn:nbn:de:0114-fqs0002204

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science*, *11*(1), 35–57. https://doi:10.1287/orsc.11.1.35.12567

Millham, M. H., & Atkin, D. (2018). Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors. *New Media & Society*, *20*(1), 50–67. Advance online publication. https://doi:10.1177/1461444816654465

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management*, *52*(6), 741–759. https://doi:10.1016/j.im.2015.06.006

Movius, L., & Krup, N. (2009). U.S. and EU privacy policy: Comparison of regulatory approaches. *International Journal of Communication*, *3*, 169–187. Retrieved from http://ijoc.org/index.php/ijoc/article/view/405/305

Newman, A. L. (2014). The governance of privacy. In D. Lēwî-Faur (Ed.), *The Oxford handbook of governance* (pp. 599–611). Oxford, UK: Oxford University Press. https://doi:10.1093/oxfordhb/9780199560530.013.0042

Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior*, *50*, 252–258. https://doi:10.1016/j.chb.2015.04.011

Petronio, S. (2002). *Boundaries of privacy*. Albany, NY: State University of New York Press.

Przeworski, A., & Teune, H. (1970). *The logic of comparative social inquiry. Comparative studies in behavioral science.* New York, NY: Wiley-Interscience.

Rainie, L. (2016). *The state of privacy in post-Snowden America*. Retrieved from http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/

Rainie, L., & Maniam, S. (2016). *Americans feel the tensions between privacy and security concerns*. Retrieved from http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, *15*(1). https://doi:10.5210/fm.v15i1.2775

Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly*, *32*(2), 129–141. https://doi:10.1016/j.giq.2015.01.003

Schwartz, B. (1968). The social psychology of privacy. *American Journal of Sociology*, *73*(6), 741–752.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1015.

Solon, O. (2018, April 4). Facebook says Cambridge Analytica may have gained 37m more users' data. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought

Trepte, S., & Masur, P. (2016). *Cultural differences in social media use, privacy, and self-disclosure: Research report on a multicultural study.* Retrieved from http://opus.uni-hohenheim.de/volltexte/2016/1218/pdf/Trepte_Masur_ResearchReport.pdf

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. *Social Media + Society*, *3*(1). https://doi:10.1177/2056305116688035

Ur, B., & Wang, Y. (2013). A cross-cultural framework for protecting user privacy in online social media. *Proceedings of the 22nd International Conference on World Wide Web*, 755–762.

Wahl-Jorgensen, K., Bennett, L., & Taylor, G. (2017). The normalization of surveillance and the invisibility of digital citizenship: Media debates after the Snowden revelations. *International Journal of*

Communication, *11*, 740–762. Retrieved from http://ijoc.org/index.php/ijoc/article/view/5523/1930

Walsh, D., Parisi, J. M., & Passerini, K. (2017). Privacy as a right or as a commodity in the online world: The limits of regulatory reform and self-regulation. *Electronic Commerce Research*, *17*(2), 185–203. https://doi:10.1007/s10660-015-9187-2

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Zhou, T., & Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Computers in Human Behavior*, *37*, 283–289. https://doi:10.1016/j.chb.2014.05.008

Appendix: Original German Quotes

Q1: Ich hab selber nicht vor, Staatsfeind zu werden, deshalb würde mir jetzt keine Möglichkeit einfallen, dass sich der Staat gegen mich wendet, . . .

Q2: So grundlegende Dinge wie Bankdaten oder so, also, oder so Online-Banking, finde ich super gefährlich.

Q3: Aber diese üblichen, ich gebe jetzt Daten an einen Dritten, Werbeanbieter zum Beispiel, weiter, damit hab ich kein Problem, weil gegen den kann man eh nichts machen.

Q4: Und, das hoffe ich, der Mensch eben dadurch nicht gläsern wird, sondern vielleicht nur aus einer bestimmten Perspektive gläsern ist.

Q5: Also ich bin dafür verantwortlich, dass ich Passwortsicherung und so etwas mache. Das wäre wie, wenn ich mein Haus nicht abschließe und jemand einbricht, dann bin ich halt Schuld.

Q6: Eigentlich habe ich das Gefühl, es sollte staatlich geregelt sein, also irgendwie von der Regierung, und weil ich das Gefühl habe, es wird nicht ausreichend gemacht, muss ich sozusagen selber nacharbeiten. Aber das nicht, weil ich das gerne möchte, sondern, weil ich das Gefühl habe, es ist unzureichend.

Q7: Da die Frage nach der Verantwortung aus meiner Sicht eine moralische ist, nein. Hier geht's, um ökonomische Unternehmen, die wirtschaftlich denken. Wenn es nach denen ginge, sollte ich denen am besten noch die Kleidergröße meiner Unterhosen schicken. Deswegen in der Verantwortung sehe ich die Unternehmen nicht. Einfach weil es der falsche Ansatz ist, diese als moralische Institution zu sehen.