Trust and Transparency in Data Protection in Online-Marketing – Differences between different Generations

Louis Kerker[a], Ingo Stengel[a], Stefanie Regier[a]

[a] *University of Applied Sciences Karlsruhe, Moltkestr. 30, Karlsruhe, Germany*

Abstract

This work aims to understand the importance of data protection for consumers of different generations. Especially under the aspects of trust and the already given options for transparency.

Trust in the services used has not emerged as a particularly important factor when it comes to using services online. The gap between the trust the consumers have in the processing of their personal data and the usage of them is too big to say that consumers really consider this point. It also became clear that consumers demand transparency and control options with regard to the processing of their data. The transparency that is currently provided is generally perceived as not being comprehensible enough and not helpful.

Keywords

Trust, Transparency, Online Marketing, Cookie Banner, Generation Z, Generation Y

1. Introduction

"Data is the oil of the 21st century". This much-quoted phrase [1], [2] makes it clear: Data is one of the most important resources of the 21st century - Big Data is on everyone's lips. In today's digital times, more and more data are coming together. In 2018, there were 33 zettabytes worldwide, it is estimated that 27% is added every year and by 2025 it is expected to be 175 zettabytes [3]. Few people can really relate to this figure, as they have no real relation to the topic. Why should they care how much the amount of data is increasing or how much data is there in the world? Because there is a non-negligible part of the huge amount of data that needs to be important to everyone. This is growing with a similar speed. This is data that companies, marketing agencies and social networks store about each of us and compile into comprehensive user profiles. Through all this data, people are increasingly becoming transparent, revealing their interests and inclinations. These can be predicted and influenced if only the right data is compiled and used, e.g. personal data is used to influence elections through targeted advertising – see the Cambridge Analytica scandal - personal data is used to target consumers with advertising. In this way, personal data is used to make money.

Especially the younger generations, the "Millenials" and "Gen Z" of our society, of which far more than 90% use social media are online for many hours every day. As "digital natives", they don't know any different. Consequently they disclose vast amounts of information about themselves and do not seem to mind.

Of course, the outrage is great when another data leak or scandal is disclosed, or when you are suddenly shown an ad for a product that you have talked about or thought about, but never actively searched for.

Online advertising is a billion-dollar market that has been growing for years and already accounts for more than 50% of global advertising spending [4]. Personal data plays an immense role in online marketing. It allows consumers to be addressed in a more targeted manner. Scattering losses are to be

CERC 2021: Collaborative European Research Conference, September 09–10, 2021, Cork, Ireland
kerkerlouis@googlemail.com (L. Kerker); ingo.stengel@h-ka.de (I. Stengel); stefanie.regier@h-ka.de (S. Regier)

avoided and advertising is to be played out more efficiently. Data, its collection and use are therefore extremely important for the advertising industry.

With this development data privacy and the protection of personal data becomes as relevant as maybe never before. But how do the consumers think about those topics? Is data privacy and the protection of their own data on their mind? Are they taking steps to protect themselves?

2. Basics

Digitalization and the increased shift of life into the online/digital space are progressing rapidly. Forms of communication and business models are changing or even being replaced, and new digital solutions are becoming established. These general digital developments do not stop at marketing. Countless new, data-driven processes have been developed in recent years [5]. Online marketing is a market worth billions and is becoming more relevant every year. According to the Zenith Forecast, spending on online advertising today already accounts for a share of more than 50% of total global advertising expenditure [4].

In its current form, online marketing is increasingly driven by the analysis of data and is thus becoming data-driven marketing [1]. Collecting data and analyzing it to make decisions is indispensable, especially in the digital field of advertising. This is because a change has taken place in online marketing in the recent past. Whereas the advertising environment used to be the focus, today the focus is on the users to be targeted. Advertising is no longer displayed on specific websites, but only to specific users who meet defined criteria [6]. This requires comprehensive knowledge about the target groups, which is obtained from user and interest profiles in which their activities and interests are collected. The information for user and interest profiles is collected primarily by tracking the activities of users, often across multiple websites. Tracking is the "collection, storage and analysis of user data and user behavior on websites"[7]. It is recorded which websites a user visits, how long he stays there and what he interacts with. From this, the interests, preferences, habits, and moods of the users are derived. Based on this, particularly targeted, personalized advertising messages are sent [8], [9]. Tracking takes place primarily through the embedding of cookies on websites or through so-called fingerprints[7].

In most of the current marketing activities, user data is of essential importance. Not only it is the basis of digital marketing, but its efficient collection and use is an essential factor for corporate success[1], [10]. Without personal data, modern business models in particular would not function successfully[11]. This is also the conclusion of the "Future Ready" study conducted by the digital agency Wundermann. In this study, 99% of the 250 respondents say that data will determine the success of marketing and sales [12]. But companies need to be aware of the risks that data processing entails. The tracking of users on their own website, but also across websites, represents a risk from a data protection perspective that cannot be neglected and for which companies should take comprehensive legal precautions[5]. Since as explained above, tracking as well as user and interest profiles are the basis for almost all significant online marketing methods and tools, this concerns the entire online marketing and its control.

General Data Protection Regulation (GDPR) was introduced to provide a regulatory framework for all these developments. GDPR is applicable throughout Europe and is partly substantiated, supplemented or modified by national laws of the member states[7], [11]. The intention of the GDPR is to replace the national data protection laws applicable and to create a uniform data protection law in the European Union[7], [11], [13]. It was created to "equip [Europe] for the digital age." According to Article 1 (1) of GDPR, the protection of individuals with regard to the processing of personal data is the object and purpose of the regulation. Through stricter regulations regarding the collection, processing, and storage of personal data, data subjects are to be strengthened in their rights vis-à-vis companies, no matter where they are located, and gain regulation over the use of their data [7], [13], [14]. In case of violations of the introduced rights and laws, the GDPR threatens with high fines. Depending on the severity of the violation, penalties of up to EUR 20 million or 4% of the total annual worldwide turnover, whichever is higher, are threatened under Article 83 (1) of the GDPR.

The processing of personal data is permitted by three permissible circumstances, which are standardized in Art. 6 (1) of GDPR. First, personal data may be processed if the consent of the data

subject has been obtained. This represents the most significant possibility for advertisers to carry out data processing in accordance with the law [7]. According to GDPR recital 32, consent must be given voluntarily, which implies that there are real choices and that consent could also be refused. It must be actively and unambiguously declared, which means that the user must also implement his or her intention to give consent by an active act and tick a box. Boxes that have already been checked or consent through inactivity do not constitute an effective declaration of consent [7], [15]. This regulation is also known as the opt-in / opt-out regulation. Consent-less cookie banners are thus no longer permitted [5]. In addition, the consent must be revocable at any time in accordance with Art. 7 (3) DSGVO. The user must be informed of the possibility of revocation before consent is given. In addition, the entire consent request must be formulated in clear and simple language [7], [15].

The next important aspect of permission for online marketing is the balancing of interests according to legitimate interest, Art. 6 para. 1 p.1 lit. f) DSGVO. According to the Conference of the Independent Data Protection Authorities of the Federal Republic of Germany and its Countries (Data Protection Conference), if consent is not given, the permissibility of advertising must be based almost exclusively on this [16]. Accordingly, data processing is lawful if the "legitimate interests of the controller or a third party [...] override the interests or fundamental rights and freedoms of the data subject which require the protection of personal data" Art. 6 para. 1 p.1 lit. f) GDPR. According to GDPR recital 47ff, direct marketing is one of the legitimate legal, economic or ideal interests of the controller. In addition, the expectation of the data subject represents an important criterion for the weighing of interests [15]. The expectation is based on the predictability of the data processing and can also be influenced by information about the data processing. Furthermore, it can be argued nowadays that the use of, for example, cookies for the display of personalized advertising can no longer be described as unexpected [7], [15], [17].

3. Related Research

The importance of privacy, protection of personal data and the effects of different types of data procession on consumers, their behavior, but also on enterprises is the subject of numerous studies, researches and scientific articles. This topic has attracted the interest of various research communities reaching from economical to psychological areas. Research has deepened since online marketing has become the dominant form of advertising, since the importance of social networks has risen immensely and since the GDPR has become effective. The reoccurring key words of those studies are trust, vulnerability and transparency.

3.1. Trust and transparency

Trust and transparency are vital factors on the success of online advertising campaigns. Bleier and Eisenbeiss [18] were using field data to demonstrate, how much the efficiency of retargeting campaigns depends on the trust a consumer has in the retailer. They compared ad impressions and click through rates (CTR) of two German retailers. The main difference of the retailers was trust. The results show, that trust has a significant impact and more trustworthy retailers can benefit from deeper personalization. The laboratory study of Bleier and Eisenbeiss [18] emphasizes the importance of trust even more. Merchants that are more trustworthy achieve significantly higher CTR with higher personalized advertising, while the CTR of less trustworthy merchants drops sharply. Customers see more personalized banner ads as not useful, experience increased reactance and privacy concerns. Not to mention the negative effects on CTR.

In addition, Beier and Eisenbeiss [18] recommend that trusted merchants should take further steps to prevent privacy concerns from arising among customers, as these lead to reactance.

Aguirre et al. [19] confirm in their study also, that „a firm's strategy for collecting information from social media websites is a crucial determinant of how customers react to online personalized advertising". They show in their first step of the experiment how different levels of personalization

have an impact on the success of the advertisement. CTR will rise above previous levels, as consumers become accustomed to data collection and seem to appreciate transparency.

The authors then conducted a study that examined the interaction of higher personalization in overt and covert data collection and the impact on CTR as well as perceived vulnerability of participants. It showed that overt data collection with higher personalization leads to a significant increase in CTR as well as a decrease in perceived vulnerability.

In a direct comparison of more or less personalized ads with overt/covert data collection on a more trustworthy website (CNN) and a less trustworthy website (Facebook) the results showed: “When firms covertly collect data and present highly personalized advertisements, customers feel vulnerable [...] and express lower click- through intentions [...] if the advertisements appear on an untrustworthy website but not if they show up on a trustworthy website” [19].

Deloitte also attributes a decisive role to trustworthiness in its study "Dataland Germany – the Transparency Gap" [20]. The authors consider it particularly important that consumers are asked for consent and that there is transparency about the use of their data. Consumers expect companies to communicate clearly, what data is used for what purposes, as well as have clear guidelines on how to handle customer data. According to Deloitte, consumers' willingness to share data does not depend crucially on the benefits they see in it, "but rather on the transparency that companies show in dealing with data."[20].

Not only Deloitte [20] recognizes transparency and control as crucial factors, but also Martin et al. [21], who even get more specific and say that transparency without control options makes customers feel "more violation and lower trust."

Trust and transparency appear to be key factors for enterprises in regard to their marketing success. Whether the consumers value transparency and trust equally when they choose their service or provider or browse the Internet is matter of the later exploration.

4. Hypotheses

With the implementation of GDPR the users received various rights and possibilities to obtain more transparency about handling of their personal data and to be in control of “the collection, storage and processing of their own data” [7]. This includes the right to information, given by Art. 15 GDPR which gives the affected user the right to know whether and to what extent personal data about them are being processed. Article 17 of the GDPR, the right to erasure, obliges the responsible party to delete personal data immediately if the data subject revokes his or her consent to processing or requests deletion. Those transparency enhancing options include also that an explicit consent, defined in Art. 6 GDPR, is necessary for data processing. This explicit consent is commonly obtained through cookie banners. In this context, cookie banners without explicit consent and the invocation of legitimate interests are no longer sufficient [5]. Possekel and Schiemann [5] state 2020 that "80 to 85 percent give their consent for cookies that are really necessary or bring convenience, but only about 20 to 40 percent of users give their consent for marketing purposes and advertising targeting and retargeting on the Internet, as well as for analytical purposes." However, Deloitte [20] recognizes among Generation Y that data protection notices are rarely read and tend to be perceived as a nuisance. This is also consistent with our own observations. Hypothesis H1 is therefore:

H1: Transparency enhancing options are appreciated but not particularly used.

Aguirre et al. [19], Bleier and Eisenbeiss [18] as well as Deloitte [20] identify trust as an important factor for the success of personalized advertisement. Facebook is used in their studies as an example of an untrustworthy website. Nevertheless, Facebook and its belonging social media and messengers (e.g. Instagram, WhatsApp) take the first two places of the top three used social medias – in each generation [22]. On top of that, scandals like the Cambridge Analytica case or data breaches are becoming much more frequent in the last years, but in her article for the Guardian Wong [23] points out that, despite of reoccurring data breaches and scandals a mass exodus from social media never happened. It is therefore

reasonable to assume that data privacy reasons and the (lack of) trust in the service / provider are not necessarily sufficient to switch. Hypothesis H2 reflects this assumption.

H2: Data privacy reasons and trust in the handling of personal data are no sufficient reasons to change the service / provider in use.

5. The Project

To answer the research question and hypotheses posed here, a quantitative research approach was chosen. This work aimed to understand the importance of data protection for consumers of the younger generations of our society as well as the feelings and preferences towards this topic. Therefore, all the results have been taken for the three different generations: Generation Z, Generation Y as well as the Generation “older” to summarize the generations born before 1980. The respondents have been addressed using a digital questionnaire that has been distributed through direct contacts as well as dedicated social media groups. This method has been chosen since the digital approach is the best way to reach respondents in younger generations. The scientific questionnaire was chosen as a survey technique because it allows capturing subjective experience in a past and private context. It can be conducted efficiently through the self-administration of the participants [24]. The respondents receive a questionnaire consisting of closed questions, which are to be answered by ticking or indicating numerical values. This type of questionnaire was chosen because the respondents can anonymously state their opinions and feelings in this format and the questionnaire is self-explanatory to fill out due to its format.

During the survey period, 243 persons participated in the data collection. Of these 243 questionnaires, however, only 198 met the predefined selection criteria for counting as valid cases. These were, among other things, the completion of the questionnaire up to the penultimate page, since no relevant questions for the study were asked on the last page. Furthermore, the data collected had to be cleaned of low-quality data. Study results suggest that lagging data can be most reliably identified by the completion time of the questionnaire [25] Therefore, the recommendations of Leiner [25] were followed to filter the completion time as an indicator of meaningless data. This is done by using the "relative completion speed" or "relative speed index" (RSI), which allows a comparison between the different questionnaires. If the RSI exceeds 2.0, the data should be viewed critically. Furthermore, the proportion of missing answers was considered. After applying these additional quality criteria, 193 questionnaires could be identified as valid and qualitatively sufficient, resulting in a sample of n=193.

It is composed of 78 male participants and 111 female participants. 3 participants did not want to specify their gender. Broken down according to age groups, the sample consists of 70 participants from Generation Z, 75 from Generation Y and 47 participants from “older” generations. The division into generations was made according to the year of birth. Participants born before 1980 were assigned to the "Older" generation. Participants born between 1980 and 1996 were assigned to Generation Y and those born in 1997 and later were assigned to Generation Z.

To compare the different types of transparency enhancing options the respondents were presented with several different cookie information / cookie banners. These are not part of this paper. They were requested to describe their interaction with cookie banners as well as with other privacy options by describing how often they use this option (never, rarely, sometimes, mostly or always).

In order to answer the question whether trust is a sufficient reason to change the provider/service in use, the participants were asked to express how big their trust or mistrust regarding the handling of their personal data is. The websites to rate are a subset of the most used social networks with some additional messengers and news websites. In a second step the participants were asked to answer how often they use the website, social network or messenger. Finally, the respondents have been asked to choose which reasons are valid reasons for them to change the service in use.

6. Results

To answer the first hypothesis, cookie banners have been chosen to represent transparency enhacing options, as the vast majority might only know those as options to change their privacy settings while

browsing. The respondents were asked to give opinions about cookie banners in general. 16% of Generation Z and 11% each of Generation Y and Generation "Older" said they read through the cookie information before making a choice. However, only 8% of Generation Y, 3% of Generation Z and 0% of the "older" generation find cookie information understandable. Just as few state that the cookie information makes the handling of data really transparent (Generation Z 6%; Generation Y 5%; Generation "Older" 4%). In contrast, 80% of Generation Z, 70% of Generation Y and 68% of the "older" generation demand that the cookie information should be more comprehensible and easier to change. Cookie information is not considered useful or helpful by any generation. Only 11% of Generation Y would agree with this. Generation Y thus represents the maximum (Generation Z 7%, Generation "Older" 9%). This is also reflected in the fact that around 2/3 of each generation would describe cookie information as annoying. The behavior of the different generations with regard to cookie information was also recorded. This is shown in the diagrams in Figures 1 a-c.

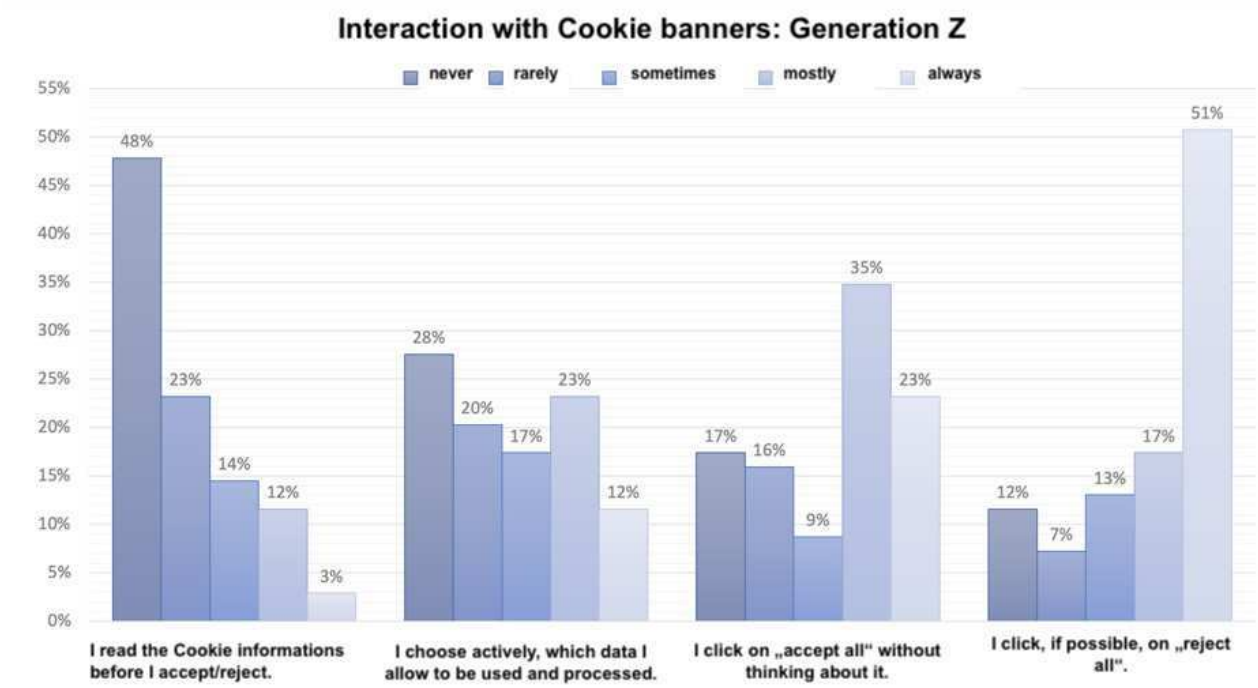

Figure 1a: Interaction with Cookie Banners: Generation Z

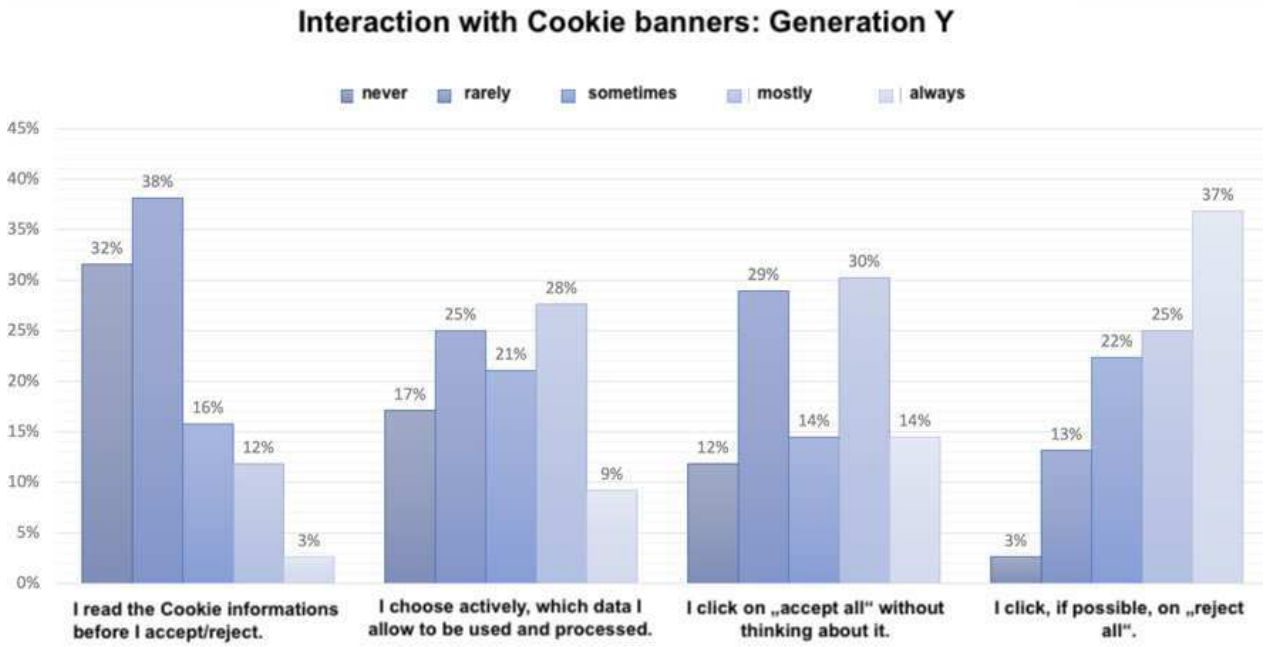

Figure 1b: Interaction with Cookie Banners: Generation Y

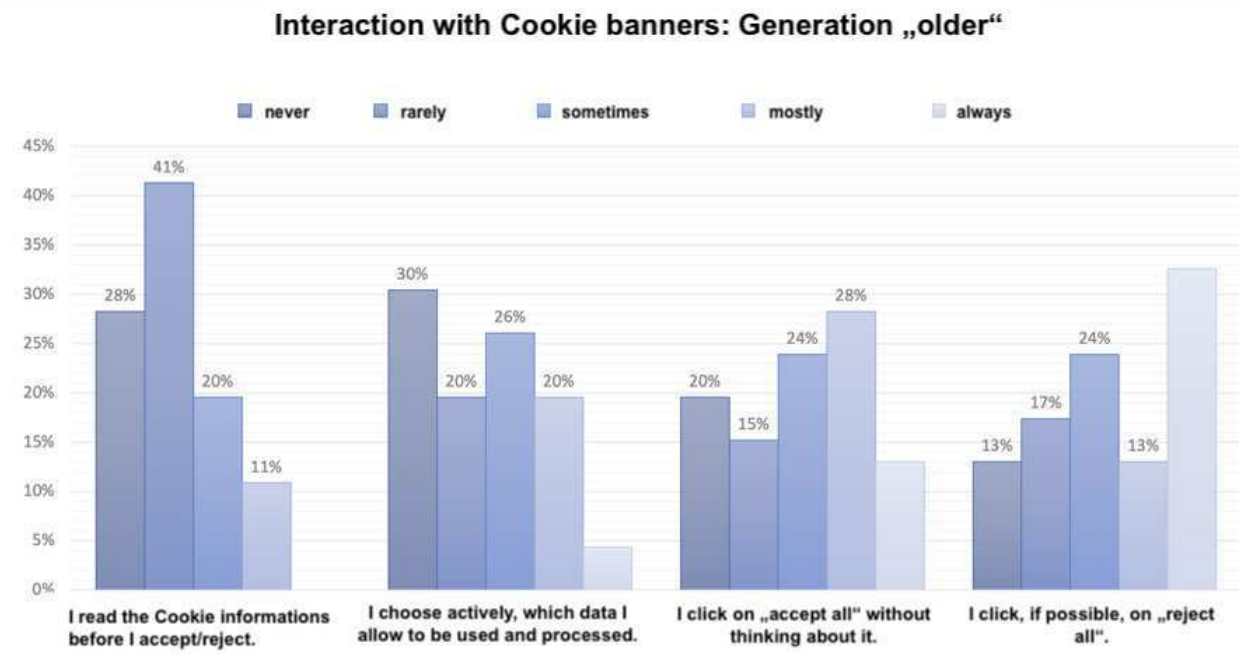

Figure 1c: Interaction with Cookie Banners: Generation “older”

It is striking that in all generations the cookie information is mostly "Never" or "Rarely" read. 69% of the "older", 70% of Generation Y and 71% of Generation Z stated this. The majority of Generations Z and Y click on "reject all" most of the time or always, if possible (Generation Z 68%; Generation Y 62%). Only 46% of the "older" generation indicated this. Approximately 1/3 of respondents from Generation Z and Y each indicated that they usually or always actively select which data may be collected. Again, fewer people from the "older" generation act in this way. Only one in four respondents stated that they usually or always actively select which data may be collected. When it comes to accepting all cookies, 58% of Generation Z usually or always click on this without thinking about it. Only 33% of Generation Z never or rarely do this. Among Generation Y, the rate of doing this most of the time or always is 44%, but 41% said they never or rarely do so. The generation "Older" achieves similar values, 35% say they never or rarely accept all without thinking about it, 41% say they do this most of the time or always. Across all generations, the number of people who read through the cookie information most of the time or always is only 11-15% (Generation Z 15%; Generation Y 15%; "Older" 11%). In contrast, around 70% of all generations stated that they never or rarely read the cookie information.

Other options which promote transparency from the consumer's point of view are also used by only a small proportion of respondents. Only 22% of Generation Z and 25% of Generation Y have already used the option to view their assigned advertising profile. Among the "older" generation, only 9% have done so. 32% of Generation Z and 33% of Generation Y said they had not done this before, but 46% / 42% had not done it because they did not know it was possible. Among the "older" 45% have not done it and 47% did not know it was possible. Requesting and downloading the collected data is also taken up by few of the respondents. Here it is only 14% of Generation Z, still 21% of Generation Y but only 6% of the "Older" generation. Here, the "not taking advantage of the possibility" among Generation Z is divided into 30% who did not and 55% who did not know it was possible. 43% of Generation Y answered "no" and 36% "no, I didn't know it was possible." Among "older" people, more than half did not know it was possible and 40% did not. The right to request deletion of collected data is also used by only a small proportion of respondents (14% Generation Z; 21% Generation Y and 4% "Older"). While only 1/3 of Generation Y and Generation "Older" respondents were unaware of the option and 43% (Generation Y) and 60% ("Older") did not use it, 46% of Generation Z did not know that it was possible and 39% did not do so. The option to deactivate personalized advertising is used by 1/3 of Generation Z respondents, not used by 1/3 and not known by 1/3. Among Generation Y, 36% deactivate personalized advertising, 28% do not do so and 7% are not aware of the option. Among the "older" respondents, 36% do not know or do not use this option and 28% deactivate personalized advertising.

To answer the second hypothesis, the first step was to learn which services and social networks are the most used by the participants.

The services and social networks most used by Generation Z are those belonging to the Facebook Group or Alphabet/Google. WhatsApp and Google (search engine, maps, etc.) share first place. They are used by 93% of the respondents belonging to Generation Z more often than four days a week. Instagram comes in second place with 80% of respondents and then YouTube with 79%. The last place of the top 5 is occupied by Snapchat with 54%.

Comparing this to the trust that users have in the service's handling of personal data shows that the most used services have the lowest percentage scores for trust. In this negative top ranking, the services belonging to Facebook again lead the way. Only 6% of the users surveyed have slight or full trust in Facebook's handling of personal data. For Facebook Messenger, the value is only 5% and Instagram also does only marginally better with 8%. The 16% of Generation Z who trust WhatsApp when it comes to handling data represent a significant improvement compared to the previous figures. However, they are also contrasted by 57% who distrust or even strongly distrust WhatsApp.

Figures 2 a-c depict the use of selected services and the trust that users have in the data processing of the respective service.

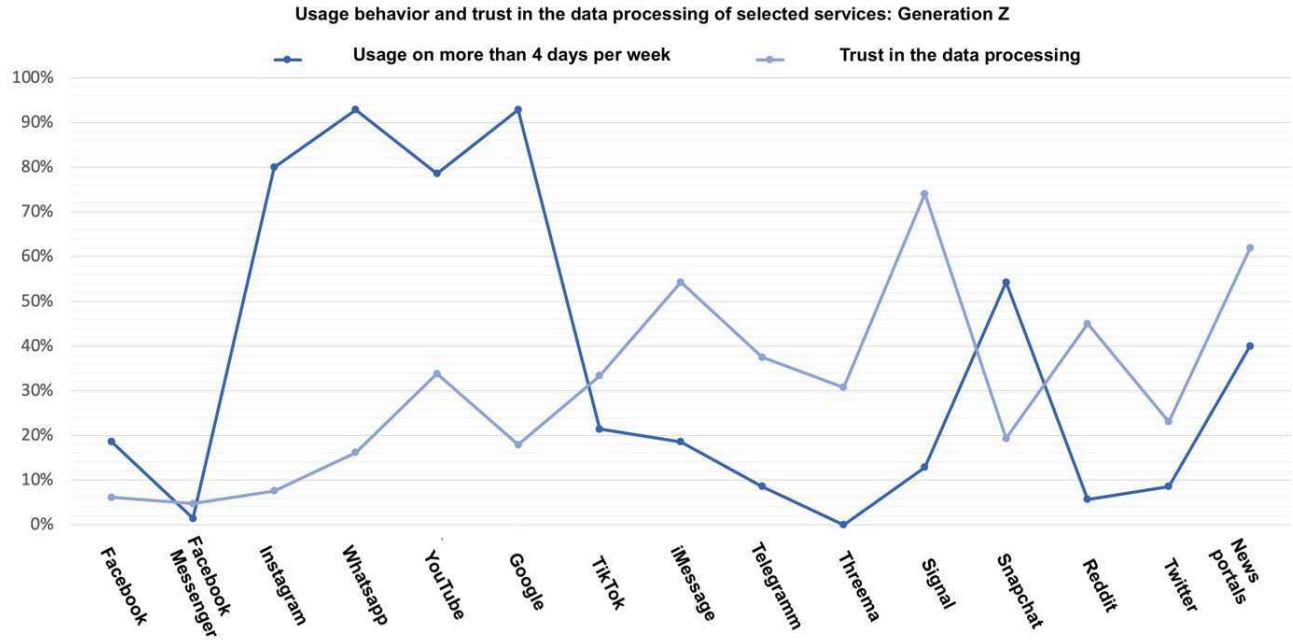

Figure 2a: Usage behavior and trust in the data processing of selected services: Generation Z

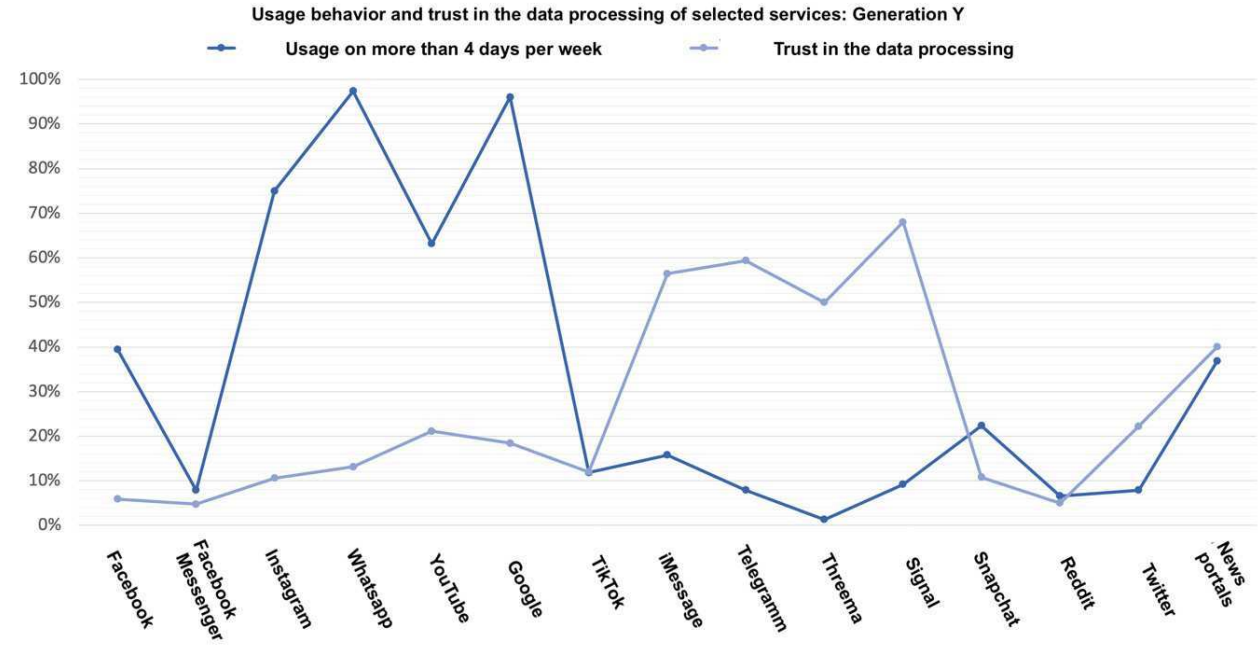

Figure 2b: Usage behavior and trust in the data processing of selected services: Generation Y

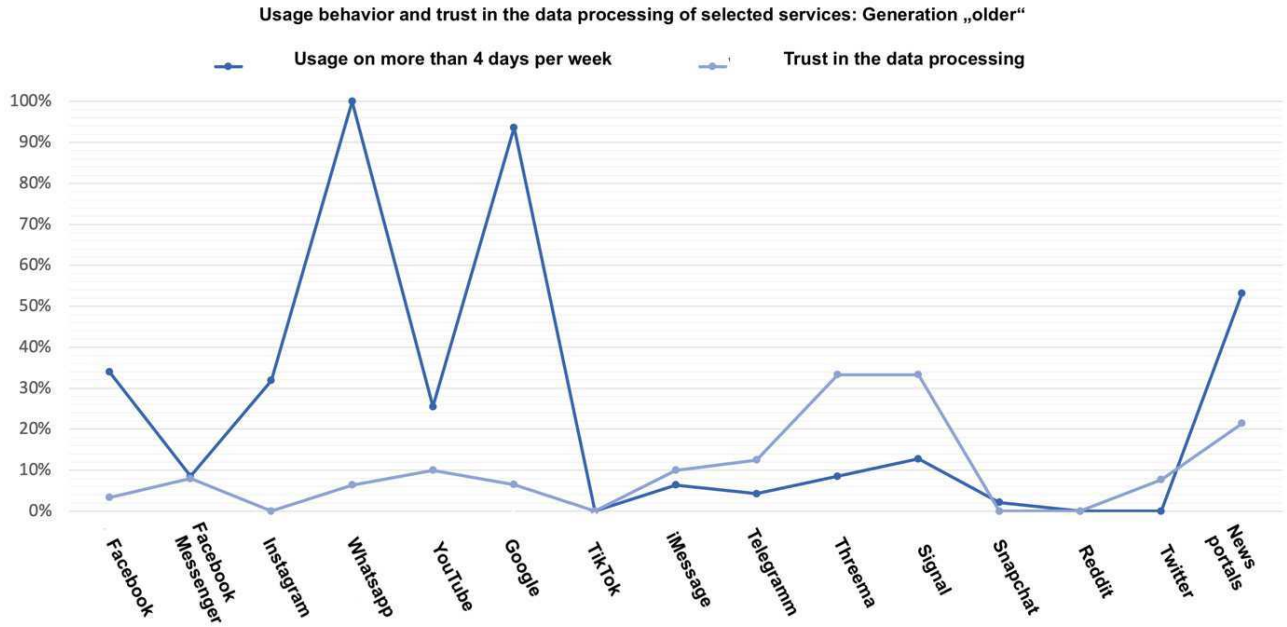

Figure 2c: Usage behavior and trust in the data processing of selected services: Generation “older”

The largest percentage of users who trust the data processing of the service is given to Signal with 74%, news portals with 62% and iMessage with 54%. While news portals are at least used by 40% of respondents more often than 4 days a week, iMessage is already used significantly less (19%) and Signal by only 13% of respondents more often than 4 times a week. Although Signal achieves the highest level of trust among respondents, it is not used at all by 80% of respondents.

Threema, which of the services available for selection can be named as one of the services with the comparatively high data protection [26], is used the least by Generation Z. Of the 70 respondents, 64 are not logged in, 4 are logged in but do not use it, and only one person uses it 1-3 days per week.

The results for Generation Y are similar. WhatsApp and Google (search engine, maps, etc.) also occupy the first two places among the respondents of this generation and are used more than 4 times a

week by 97% and 96%, respectively. This is followed by Instagram (75%), YouTube (63%) and Facebook (39%). Generation Y distrusts Facebook and Facebook Messenger the most, analogous to Generation Z (76% / 78%). Unlike Generation Z, however, TikTok (64%), Instagram (58%) and Snapchat (57%) follow.

Generation Y, like Generation Z, has the least trust in the services belonging to Alphabet/Google and Facebook when it comes to handling personal data. YouTube still receives the highest value here, with 21% of users stating slight to full trust (FB 6%, FB Messenger 5%, Instagram 11%, WhatsApp 13%, Google 18%).

The messengers Signal, Threema, Telegram and iMessage receive the most trust from users in handling data. Signal receives 68%, iMessage, Telegram and Threema between 50% and 59%. It is surprising that, as with Generation Z, the services with the highest trust are not among the most used services.

Among the "older" generation, news portals are used most frequently after WhatsApp and Google. Only then, Facebook, Instagram and YouTube follow. It is unusual that among the "older" generation, only Signal and Threema are trusted by more than 30% of users. Even with these two messengers, distrust about the handling of personal data is over 10 percentage points higher than trust. Twitter, Reddit and Snapchat in particular score exceptionally poorly in terms of trust scores. However, these services are also the least used by the respondents of this generation. The much-used news portals achieve a medium level of trust. The relatively heavily used services Facebook, Instagram and WhatsApp score high values for distrust, analogous to the two younger generations. A maximum of 10% of users said they had confidence in the data processing of these services. On average, 31% of Generation Z, 27% of Generation Y and 10% of the "older" generations say they have at least slight trust in the services' handling of personal data.

When asked directly whether users use services even though they have concerns about data privacy, a consistent picture emerges across all generations. 45% of respondents from Generation Z fully agreed to use services even though they had concerns about data privacy. The figure for Generation Y was 50% and for the older generations 51%. If the proportion of people who tend to agree with this statement is also added, the result is 87% for Generation Z, 87% for Generation Y and 89% for the older generation. After a Chi Square Test for independence, it can be seen that there is no stochastically significant correlation between "generation" and "use of services despite data protection concerns".

7. Discussion

Hypothesis H1 assumes that opportunities to promote transparency are valued, but not actually used. To prove this hypothesis, the right to information under Article 15 and the right to delete one's own data were used as examples of such transparency-promoting measures. The use of cookie banners was also queried, as this is probably the most universally known means by which consumers can track their data processing or restrict data processing. Aguirre et al. [19], Bleier and Eisenbeiss [18], and Deloitte [20] identified both transparency about data processing and trust as key factors. As Table 1 shows, there are differences between the generations. Generations Z and Y generally rated the cookie banners available for selection slightly better than the "older" generation. It is noticeable that the cookie banners with a high level of information or transparency about the use of data did not necessarily receive the best rating. The best ratings in each case in all generations were given to the cookie banners that have only a medium level of information content, but offer several different options for selecting which data may be processed directly, offer better selection options than "accept all" or have additional settings set up that are not, however, directly mapped. It is also noticeable that a cookie banner with little information receives a relatively good rating if it has "Accept all" and "Reject non-essentials" as default selections. The cookie banners with the most detailed information and thus the highest transparency about data processing did not achieve exceptionally good ratings. It seems as if the options to limit the data processing are more important than a detailed explanation.

The reason for this can be inferred from other survey results. With a share of only 16%, Generation Z was the generation whose most users read through the cookie information before selecting it at all. Conversely, this means that the vast majority do not read the information. Even if the information were

actually read, very few would find the information clear and understandable or would find that it makes transparent how the data is handled. Most respondents found it annoying and unhelpful. These findings were also similar to those drawn from the survey by Deloitte [20] and can therefore be seen as confirmed.

Most respondents of the younger generations also click on "Reject all" most of the time to all of the time, if possible. Across all generations, the selection options are not considered sufficient. More than 2/3 of the "older" generation, 70% of Generation Y and even 8 out of 10 Generation Z respondents also demand that the cookie information should be easier to understand and change. Since the majority of all generations also feel that the cookie information does not make transparent what happens to the data, the following conclusion can be drawn:

Transparency is valued. In its current form, however, cookie information does not provide the transparency that consumers want. Even detailed information does not provide the transparency that would be necessary, because consumers find cookie banners annoying, rarely read them at all, and when they do read them, do not understand them sufficiently. Therefore, the banners that are rated better are those that provide just enough to understand what is most important. It can also be concluded from the present results that control options are more important to the respondents than transparency.

The other transparency-promoting options, such as the rights stemming, from Articles 15 and 17 of GDPR to obtain information about the data collected or to have it deleted, are used by few users. They tend not to be used because they are not viewed positively, but because the majority of users of all generations do not know that these options exist.

Hypothesis H1 and the research findings of Deloitte [20], Acquisti et al. [19] and Bleier and Eisenbeiss [18] as well as Martin et al. [21], who consider transparency with additional control options to be extremely important, can therefore be confirmed.

Hypothesis H2 states: "Data protection reasons and trust in the handling of personal data alone are not sufficient to switch services/providers. As explained in section Related Research Aguirre et al. [19], Bleier and Eisenbeiss [18] and Deloitte [20] in particular identified trust as a key factor. Aguirre et al. [19] and Bleier and Eisenbeiss [18] relate this more to the context of the effectiveness of advertisements and Deloitte [20] to the willingness to share data. The present research extends this approach by asking whether trust is also such an important factor that can cause users to turn their backs on services and providers. The results presented here paint a clear picture across all generations: for all generations, social networks of the Facebook Group are among the most used services. The fact that Facebook has a questionable reputation when it comes to the use of data is shown not only by the research of Cabañas et al. [27], but also by Aguirre et al. [19], which lists Facebook as an untrustworthy website. The users surveyed feel the same way. Only a vanishingly small proportion of all three generations express their trust in these social networks or services. However, the astonishing findings of the survey are only revealed in the next step, when the trust that users place in these services is compared with the extent to which these services are used. It becomes apparent that none of the most frequently used services receives a high rating in this regard. Rather, it becomes clear that the social networks or messengers that are given a high trust rating have very low usage rates across all generations. In addition, it could be shown that the overwhelming majority of respondents, stochastically independent of generation, state that they use services despite data privacy concerns. This is despite the fact that an even larger proportion of respondents in each generation stated that they saw data protection reasons as a reason to switch providers. If the environment was seen as a primary reason for switching services for all generations, this could explain why the highest usage rate does not correlate with the level of trust that exists in providers. Since the majority of the environment uses the service and does not switch, the individual consumers also use this service despite the lack of trust.

Although the proportion of respondents who see data privacy as a reason for switching is high in all generations, it continues to rise with increasing age. A stochastically significant correlation between age and data protection as a reason for switching was demonstrated. The present results can neither confirm nor disprove the research findings of Aguirre et al. [19] or Bleier and Eisenbeiss [18] regarding the influence of trust on the effectiveness of advertising measures. However, they can extend them to the effect that privacy reasons and trust can be seen as important influencing factors on consumer behavior, but do not influence the actual behavior of consumers regarding their choice of service or provider. Thus, Wong [23] can be confirmed to the effect that, despite recurring data leaks, there has not yet been a mass exodus from social networks, and this despite the fact that in the present survey

about 2/3 of each generation stated that data leaks were the reason for switching. It is interesting that the environment is the more decisive reason for a change. This was indicated by most of the respondents across all generations. It was found that the respondents' environment has a major influence on behavior. This is consistent, especially with respect to Generation Z, with the findings of current research [28]. It showed the significant influence of friends and family or the environment on actions and use of services.

Hypothesis H2, that data protection reasons and trust in the handling of personal data are not sufficient reasons to switch providers, can thus be confirmed.

8. Conclusions and Outlook

This worked aimed to understand the importance of data protection for consumers of different generations. Especially under the aspects of trust and the already given options for transparency.

The results have shown that trust in the services used has not emerged as a particularly important factor when it comes to using services online. The gap between the trust the consumers have in the processing of their personal data and the usage of them is too big to say that consumers really consider this point. In general, data protection reasons are one reason for switching providers. This applies to all consumers, but a correlation between age and this reason could be demonstrated. For the "older" consumers, this was a stronger argument than for the younger ones. Nevertheless, all generations use services despite their privacy concerns. It was shown that it is primarily the consumer's environment that influences which services are used. It also became clear that consumers demand transparency and control options with regard to the processing of their data. The transparency that is currently provided is generally perceived as not being comprehensible enough and not helpful.

9. References

[1] S. Boßow-Thies, C. Hofmann-Stölting, and H. Jochims, *Data-driven Marketing: Insights from Wissenschaft und Praxis*. 2020.

[2] C. Höinghaus, 'Daten: Das Öl des 21. Jahrhunderts: Big Data wirtschaftlich sinnvoll einsetzen', Aug. 28, 2015. https://www.cio.de/a/big-data-wirtschaftlich-sinnvoll-einsetzen,3246278 (accessed Jul. 30, 2021).

[3] M. Kroker, 'Weltweite Datenmengen sollen bis 2025 auf 175 Zetabytes wachsen – 8 mal so viel wie 2017', Nov. 27, 2018. https://blog.wiwo.de/look-at-it/2018/11/27/weltweite-datenmengen-sollen-bis-2025-auf-175-zetabyte-wachsen-8-mal-so-viel-wie-2017/ (accessed Jul. 26, 2021).

[4] H. Rampe, 'Zenith Forecast: 2021 fließt die Hälfte aller Werbespendings in Internet-Werbung', *https://www.horizont.net*, Jul. 09, 2020. https://www.horizont.net/medien/nachrichten/zenith-forecast-2021-fliesst-die-haelfte-aller-werbespendings-in-internet-werbung-176029 (accessed Jul. 26, 2021).

[5] M. Possekel and S. Schiemann, 'Data-driven Marketing als Risiko', *Control Manag Rev*, vol. 64, no. 2, pp. 52–57, Feb. 2020, doi: 10.1007/s12176-019-0079-5.

[6] I. Kamps and D. Schetter, *Performance Marketing Der Wegweiser zu einem mess- und steuerbaren Online-Marketing - Einführung in Instrumente, Methoden und Technik*. 2020. Accessed: Jun. 25, 2021. [Online]. Available: https://doi.org/10.1007/978-3-658-30912-1

[7] M. Lutz, 'Datenschutz im Onlinemarketing', in *Datenrecht in der Digitalisierung*, L. Specht-Riemenschneider, N. Werry, and S. Werry, Eds. Erich Schmidt Verlag, 2020, pp. 203–250.

[8] N. Fabisch, 'Ethische Grenzen der Datennutzung im Marketing', in *Data-driven Marketing*, S. Boßow-Thies, C. Hofmann-Stölting, and H. Jochims, Eds. Wiesbaden: Springer Fachmedien Wiesbaden, 2020, pp. 283–312. doi: 10.1007/978-3-658-29995-8_13.

[9] M. Nebel, 'Privatsphäre und Privatheit', in *Persönlichkeitsschutz in Social Networks: Technische Unterstützung eines grundrechtskonformen Angebots von Social Networks*, M. Nebel, Ed. Wiesbaden: Springer Fachmedien, 2020, pp. 39–51. doi: 10.1007/978-3-658-31786-7_4.

[10] H. M. Wolters, 'Qualität von Kundendaten – Ansätze zur Analyse und Verbesserung als Basis für effiziente Marketingentscheidungen', in *Data-driven Marketing*, S. Boßow-Thies, C. Hofmann-Stölting, and H. Jochims, Eds. Wiesbaden: Springer Fachmedien Wiesbaden, 2020, pp. 29–41. doi: 10.1007/978-3-658-29995-8_2.

[11] C. Westerkamp, 'Datenschutz gemäß DSGVO im datengetriebenen Marketing – ein Überblick', in *Data-driven Marketing*, S. Boßow-Thies, C. Hofmann-Stölting, and H. Jochims, Eds. Wiesbaden: Springer Fachmedien Wiesbaden, 2020, pp. 237–256. doi: 10.1007/978-3-658-29995-8_11.
[12] D. Hein, 'Wunderman-Studie: Zwei Drittel aller Unternehmen können aus Daten keine Marketing-Maßnahmen ableiten', *https://www.horizont.net*, Mar. 13, 2018. https://www.horizont.net/marketing/nachrichten/Wunderman-Studie-Zwei-Drittel-aller-Unternehmen-koennen-aus-Daten-keine-Marketing-Massnahmen-ableiten-165526 (accessed Jun. 25, 2021).
[13] T. Becker, A. Freiherr von Bussche, J.-M. Grages, and A.-M. Frey, *DSGVO/BDSG : Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG*, 3. Köln: Verlag Dr. Otto Schmidt KG, 2018.
[14] J. Behrens, 'DSGVO im Digitalen Marketing – heutige und künftige Herausforderungen für den CMO', in *Digitales Marketing – Erfolgsmodelle aus der Praxis*, M. Terstiege, Ed. Wiesbaden: Springer Fachmedien Wiesbaden, 2020, pp. 17–42. doi: 10.1007/978-3-658-26195-5_2.
[15] U. Schläger, J.-C. Thode, C. M. Borchers, C. S. Conrad, and M. Cyl, Eds., *Handbuch Datenschutz und IT-Sicherheit*. Berlin: Erich Schmidt Verlag, 2018.
[16] DSK, 'Kurzpapier Nr. 3', presented at the Konferenz der unabhängigen Datenschutzbehör- den des Bundes und der Länder (Datenschutzkonferenz), 2017.
[17] R. Schwartmann, A. Jaspers, G. Thüsing, D. Kugelmann, M. Atzert, and A. Buchmann, *DS-GVO/BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*. Heidelberg: C.F. Müller, 2018.
[18] A. Bleier and M. Eisenbeiss, 'The Importance of Trust for Personalized Online Advertising', *Journal of Retailing*, vol. 91, no. 3, pp. 390–409, Sep. 2015, doi: 10.1016/j.jretai.2015.04.001.
[19] E. Aguirre, D. Mahr, D. Grewal, K. de Ruyter, and M. Wetzels, 'Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness', *Journal of Retailing*, vol. 91, no. 1, pp. 34–49, Mar. 2015, doi: 10.1016/j.jretai.2014.09.005.
[20] Deloitte, 'Datenland Deutschland Studie - Die Transparenzlücke', *Deloitte Deutschland*, 2014. https://www2.deloitte.com/de/de/pages/trends/studie-datenland-deutschland.html (accessed Jul. 26, 2021).
[21] K. D. Martin, A. Borah, and R. W. Palmatier, 'Data privacy : effects on customer and firm performance', *Journal of marketing*, vol. 81, no. 1, Jan. 2017.
[22] Adobe, Ed., 'Adobe Across the Ages Study - Vertrauen in Marken und Medien: Worauf es den Konsumenten unterschiedlicher Generationen wirklich ankommt.' Aug. 2019.
[23] J. C. Wong, 'The Cambridge Analytica scandal changed the world – but it didn't change Facebook', *the Guardian*, Mar. 18, 2019. http://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook (accessed Jun. 25, 2021).
[24] N. Döring and J. Bortz, *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften*, 5. vollständig überarbeitete, Aktualisierte und erweiterte Auflage. Berlin Heidelberg: Springer, 2016.
[25] D. J. Leiner, 'Too Fast, too Straight, too Weird: Non-Reactive Indicators for Meaningless Data in Internet Surveys', *Survey Research Methods*, pp. 229-248 Pages, Dec. 2019, doi: 10.18148/SRM/2019.V13I3.7403.
[26] I. Bauer, 'Wie sicher ist Threema?', *heise online*, Apr. 21, 2021. https://www.heise.de/tipps-tricks/Wie-sicher-ist-Threema-5043167.html (accessed Jul. 12, 2021).
[27] J. G. Cabañas, Á. Cuevas, A. Arrate, and R. Cuevas, 'Does Facebook use sensitive data for advertising purposes?', *Commun. ACM*, vol. 64, no. 1, pp. 62–69, Jan. 2021, doi: 10.1145/3426361.