IADIS International Journal on WWW/Internet
Vol. 17, No. 1, pp. 1-13
ISSN: 1645-7641

PRIVACY CONCERNS OF DIGITAL NATIVES: DIGITAL ABOVE ALL?

Barbara Engels
German Economic Institute, Cologne, Germany

ABSTRACT

Data is the main resource of the digital economy. Accordingly, personal data constitutes the exchange value for the use of numerous online services such as social media. Many Internet users willingly disclose their data to these services. Oftentimes, there exists a discrepancy between individual privacy preferences and actual behavior. Against this background, this study examines the preferences of the so-called digital natives for privacy. 3,000 students aged between 14 and 21 in Germany were asked about their use of social media and their privacy preferences for these online services. In addition, their willingness to pay for privacy-friendly online services is analyzed. The study shows that while privacy is important to many digital natives, most are not willing to pay for it.

KEYWORDS

Privacy, Data, Networks, Digitalization, Social Media

1. INTRODUCTION

Data is the main resource of the digital economy. Accordingly, many companies strive for more and more data. 90 percent of Google's revenue and 95 percent of Facebook's revenue, for example, can be accounted to advertising based on personal data analytics (Pollack, 2016). The disclosure of personal information is the exchange value for the use of numerous online services.

Concern about the lack of data protection is generally very high (European Commission, 2015). Only three percent of German Internet users do not care what happens to their data on the Internet (Bitkom, 2015). However, many Internet users readily disclose their personal data. 87 percent of the Internet users in Germany use online services that collect their personal data, even though they do not have full confidence in the data protection provided by these services (Bitkom, 2015). This constitutes the so-called privacy paradox. A systematic review of the literature on this phenomenon is provided by Barth and de Jong (2017).

Engels and Grunewald (2017), Taddicken (2013), Keith et al. (2013), Sutanto et al. (2013), Acquisti and Gross (2006) and Hann et al. (2002) also deal with the privacy paradox. There are various explanations for the fact that although privacy is considered important, this is not necessarily reflected in the behavior of users. Among other things, a lack of rationality, ignorance, context dependency and the formability of preferences play a role: Acquisti et al. (2016) find that stated preferences generally differ from observed behavior and that people's attitudes to data protection are subjective, context-dependent and dynamic, i.e. time-dependent.

For example, because of a high level of present preference, Internet users perceive immediate rewards from online services and data sharing as more important than discounted future consequences (O'Donoghue/Rabin, 2000). The benefits are more immediate than the costs that are often only noticed ex post. A lack of knowledge about the extent to which data is stored and used, and how to protect this data, also leads to inconsistent online behavior. Two thirds of German Internet users state that they lack information about what they themselves could do to protect their data on the Internet (Bitkom, 2015).

Distorted perceptions influence how much value users place on data protection. The perception of a violation of privacy depends strongly on the context (Nissenbaum, 2009). Acquisti et al (2015) show that people are more likely to disclose information if they observe that their environment does the same. This can explain the high willingness to disclose personal data such as photos and other postings in social networks.

Many Internet users follow a simple cost-benefit calculation when it comes to privacy, where the perception of costs and benefits is often distorted. They may be willing to pay for a more privacy-friendly service if it offers significant added value and there is confidence in the service (Schreiner/Hess, 2015). The advantages of data disclosure are weighted higher in the privacy paradox than the threat to privacy (Engels/Grunewald, 2017). The assessment of the importance of data protection is therefore not absolute but can be controlled by economic incentives (Hann et al., 2002). The willingness to pay for data protection and data protection criticism or data protection preferences are often not consistent with each other.

Against this background, this study examines the preferences of digital natives for privacy. It is believed that through early and continuous contact with online services, young people are more likely to be able to assess privacy preferences and choose respective settings in online services (Blank et al., 2014). 89 percent of the 12 to 19-year-olds in Germany are online every day, regardless of gender, age or education (Mpfs, 2018, 30). They grow up with digitalization and the Internet. They meet and connect in social networks and communicate via digital services. They leave digital traces through their online behavior, which build up over the years to large data sets and are hardly erasable.

Based on a survey of 3,000 students aged between 14 and 21 in 2017 in Germany, digital natives' use of social media and networks, referred to as social online services, and their privacy preferences for these online services are analyzed. In addition, the willingness to pay for privacy-friendly online services is determined.

The contribution of this paper is hence a close analysis of the Internet privacy preferences of a part of society that should be very familiar with the Internet. It is the first empirical evidence of the existence of the so-called privacy paradox among digital natives in Germany.

2. RESULTS

2.1 Dataset

The analyzed sample consists of 3,000 students between the ages of 14 and 21 (so-called digital natives) from all over Germany, including 1,530 girls and 1,470 boys. 76 percent of the respondents are students from a secondary school (Gymnasium), 11 percent are from vocational schools, and 6 percent from comprehensive schools. Thus, the sample does not represent the population of all students but contains an above-average number of students from schools allowing higher education. All respondents participated in the JUNIOR program in the 2016/2017 school year. At the heart of the JUNIOR program is the creation of a student company (JUNIOR, 2018). Accordingly, the sample mostly consists of students interested in business. The survey was part of the final evaluation of the program. This form of survey comes with some shortfalls and limitations, see 2.5. Most respondents are 17 years old (figure 1). The sample is not representative. A generalization of the results of the study is therefore not possible. Nevertheless, the results provide valuable indications.

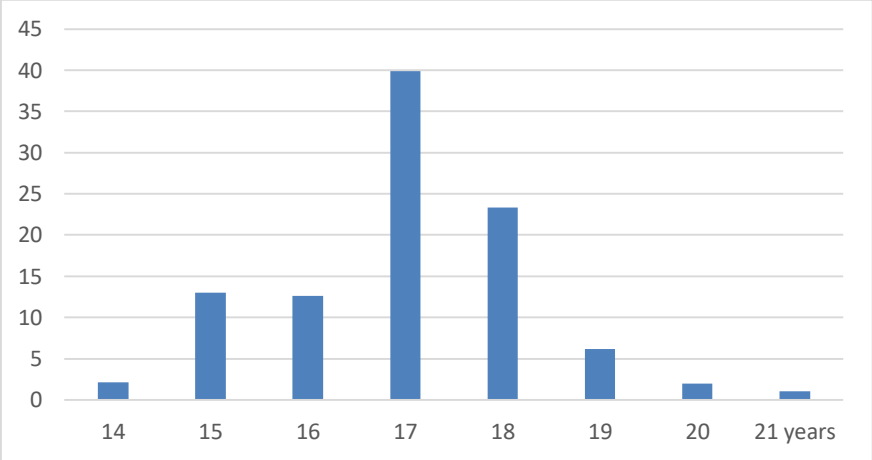

Figure 1. Age of respondents. Share of age group, in percent. N=3,000

The analysis included the online services WhatsApp, Snapchat, Skype, Facebook, Twitter, Instagram, Youtube, Google+, Pinterest, Flickr and Tumblr. They are assigned to categories that describe their main function. The three categories are neither mutually exclusive nor fully comprehensive. Many of the services can be assigned to more than one category.

Accordingly, WhatsApp, Snapchat and Skype are communication services whose main function is the often bilateral exchange of messages. Instagram, Pinterest, Google+ and Facebook are social networks, i.e. networks that serve to connect many users via text or images. Youtube, Twitter, Tumblr and Flickr are regarded as platforms that bring together providers and consumers of different media and formats (media platform).

Depending on the service category, network effects and thus potential lock-in effects are very different (see Evans/Schmalensee, 2007). Social networks and communication services have very high network effects, while media platforms have less strong network effects (Engels,

2016). Strong network effects mean that users of a service are more likely to remain with a certain service, even if they have data privacy concerns, because their entire network, their social environment, also uses this service. For the users of Instagram, for example, contact with the individual environment is very important: 82 percent of young users follow people they know personally (Mpfs, 2018, 37). Stiftung Neue Verantwortung (2017, 24) commented on network effects: "However, in theory, it may also be possible to avoid certain online services, which in practice often equates to a refusal of the modern world eo ipso. Even if there are alternative, privacy-friendly services, the network effects of other services are so strong that consumers will always be disadvantaged if they do not use them."

For media platforms, network effects are less pronounced: It plays a minor role for a user whether her social environment watches videos rather on Youtube or on another platform such as Vimeo. Her individual benefit of using Youtube changes, if at all, only marginally.

Between the service categories, but also within the categories, the extent to which data is stored and reused differs dramatically. Particularly social networks are very data intensive. The benefit of using the service is positively correlated with the amount and diversity of personal information that the user discloses. In addition, a relatively high level of minimum information is required to use the service at all. While the media platform Youtube can also be used without registration, the social network Pinterest only works if a personal account is opened. Within social networks, Facebook is more data intensive than Pinterest.

Internet users' trust in social networks when handling personal data is very low: In a representative survey, only 15 percent of respondents expressed their trust in these services (Bitkom, 2017). In fact, around 95 percent of Facebook's sales are due to the fact that personal data is not only used to improve the service for users, but also and above all to pass it on to advertising partners (Pollack, 2016).

Communication services mainly access the contact lists of users. The storage and processing of the data happens in the background: the consumer does not realize that her data is used because the service provided is not influenced ore altered by it. This distinguishes communication services from social networks like Facebook, for example, where personalized advertising indicates to the consumer that her personal information is being used.

Hence, the role that personal data plays in the primary business model of online services varies widely. It can be assumed that the input and analysis of personal data in social networks increases the utility of these more than the input of personal data in communication services. Media platforms are in-between: Although the analysis of user behavior allows a more accurate service, it is possible to use them without it. The observable added value is essential for the evaluation of data collection and data use by the user. Li and Unger (2012) show that, under certain circumstances, users soften their privacy concerns if they experience a highly customized service (personalization). This is especially the case when online services openly address their data policy, thereby establishing trust. According to Bitkom (2015), users are pragmatically committed to privacy: nearly three-quarters of respondents in this survey indicate that the ease-of-use of online services should not suffer from excessive privacy rules. More than half (58 percent) think that it is good if the services are easier to handle through the use of personal data.

The implications of data storage, data processing, and data combinations are so complex that it is virtually impossible for individuals to adequately assess the consequences of consenting to the use of data by a service (Stiftung Neue Verantwortung, 2017, 24). Nissenbaum (2009) speaks of the loss of "contextual integrity": For a consumer, it is usually not comprehensible why the use of a service (and therefore of personal data) in one context could have consequences in a completely different context.

2.2 The use of Social Online Services

The use of social online services is widespread among the surveyed students. 86 percent use at least one of the considered services (figure 2). Most of the surveyed students use three or four of the services. Overall, 78 percent of respondents use multiple services in parallel. Only 14 percent do not use any of the services. Whether they do this for privacy reasons, is not apparent from the survey. 46 percent of respondents were classified as so-called heavy users. They claimed to use at least four of the eleven services.

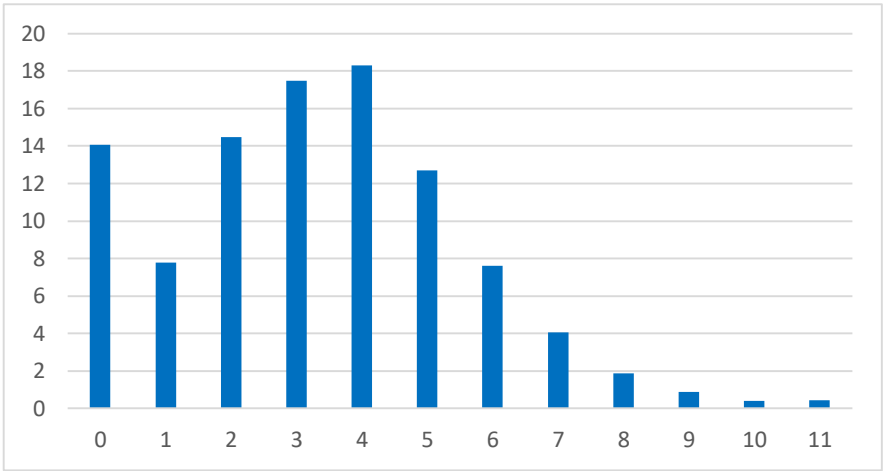

Figure 2. Parallel use of social online services. Share of respondents that use the respective number of social online services, in percent. N=3,000

The communication service WhatsApp is most widely used (78 percent), followed by the communication service Snapchat (see figure 3). The image and video platform Flickr is hardly used. Facebook is also at the bottom of the list with 17 percent. The most popular services belong to the category of communication, followed by social networks and media.

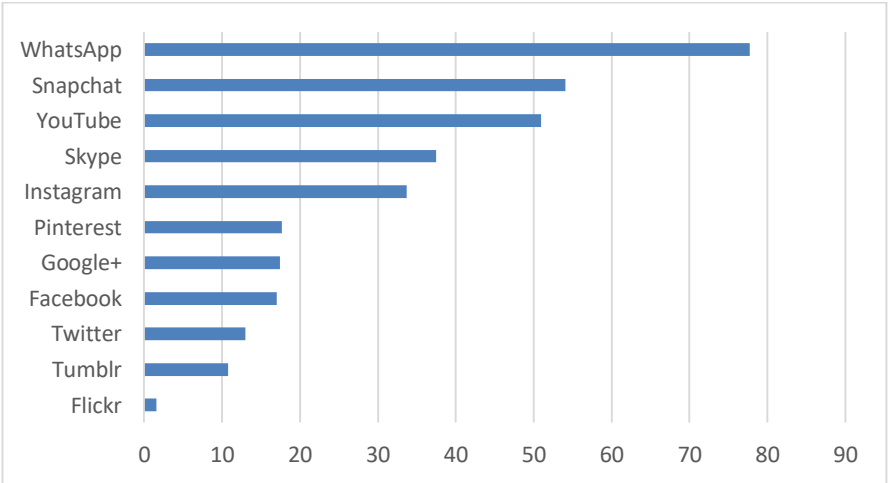

Figure 3. Use of social online services. Share of respondents that use the respective online service, in percent. N=3,000

2.3 Privacy Preferences

The majority of the surveyed students does not like that the social online services store and use their data. This is especially the case for the services that are popular among the students. 67 percent of the respondents dislike that WhatsApp stores and uses their personal data, for Snapchat the figure amounts to 63 percent (figure 4). Students do not care about the use of personal data by online services they do not use frequently.

When interpreting these values, it should be noted that the applications store and reuse data to varying extents and with different visibility for the user (see 2.1). Media coverage also has an effect on the perception of privacy friendliness. In the survey, it was not pointed out to what extent the respective services are, from an objective point of view, privacy-friendly or not.

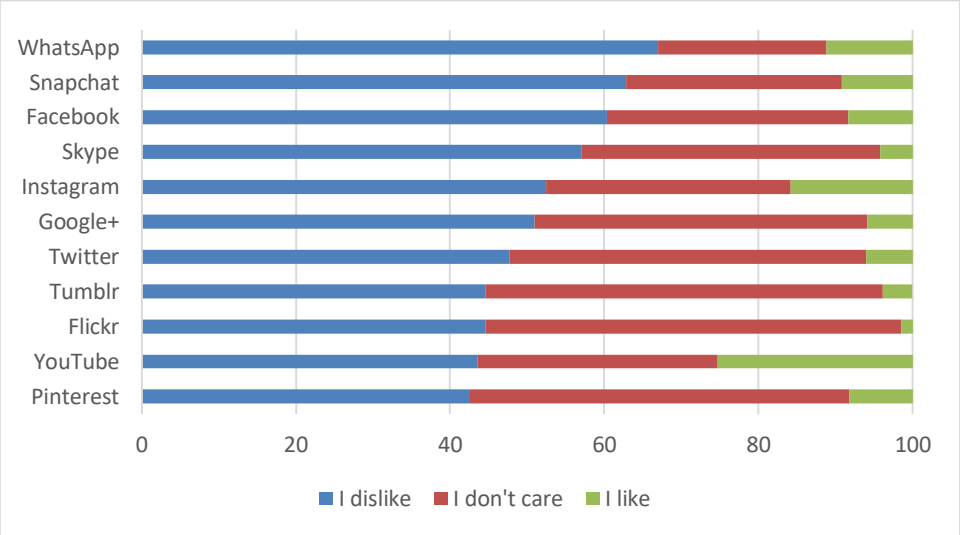

Figure 4. Assessment of personal data use. Share of respondents that dislike/do not care/like that the respective online service uses their personal data, in percent. N=3,000. Based on the survey question: “Companies like YouTube, Facebook, Snapchat, and so on can store and later reuse messages we write, websites we visit, and the things we search for online. Accordingly, my personal information is stored and used. For example, it's sold to other companies or used to show appropriate advertising. That the following social media services store and use my data, I like/ I dislike / I don't care about"

Only 20 respondents (0.7 percent) replied that they like the use of personal data by all considered services. In contrast, 792 respondents (26 percent) dislike the use of personal data by all services. There are hardly any students who find it invariably good what happens to their data. But there are many who are indifferent.

Overall, 73 percent of respondents are considered critical of personal data usage by online services (hereafter referred to as "aware"; see table 1). For this classification, the assessment of the use of the data by the different services was aggregated and an average was calculated. An assessment of data use with "I like" was given a rating of 1, "I don't care" with two and "I dislike" with three. Respondents that tend to "I dislike" (average value greater than 2.0), are classified as "aware". They are aware of the use of data by the services and are critical of it. Many respondents are especially critical of data exploitation by communication services. Regarding media platforms, the respondents are less critical. In this case, the relationship between the critics and the non-critics is almost a balance. Overall, criticism of the most

frequently used category of communication services is significantly higher than that of the least used service category media.

Table 1. Awareness according to social online service category. Share of respondents that consider the use of data as critical or uncritical, in percent of all respondents; N=3,000

	Communication services	**Social networks**	**Media platforms**	**Total**
Critical/ aware	74	64	55	73
Not critical/ not aware	26	36	45	27

A critical assessment of the use of data by the services usually does not result in the services not being used. Both users and non-users criticize the lack of data protection (figure 5). In the case of the WhatsApp, Snapchat and Skype communication services, the users are more critical of the lack of data protection than the non-users. For all other services, the non-users are more critical than the users. In the case of communication services, the lack of data protection does not seem to lead to a waiver of the service.

For Twitter, Tumblr, and Flickr, users like the fact that their data is used significantly more than non-users, the same accounts for Pinterest. The lead for Snapchat, Skype, Instagram, Google+ and Facebook is less pronounced. In the cases of WhatsApp and Youtube, particularly non-users dislike their data exploitation. It can be concluded that the respondents notice the benefits that the use of personal data by Twitter, Tumblr, Flickr and Pinterest creates for them. Data usage potentially makes these services meet the personal user needs in a better fashion. Even Snapchat, Skype, Instagram, Google+ and Facebook seem to be able to create an additional benefit through data usage, which is perceived by the users. For WhatsApp and Youtube, this added value does not seem to be perceived to a large extent.

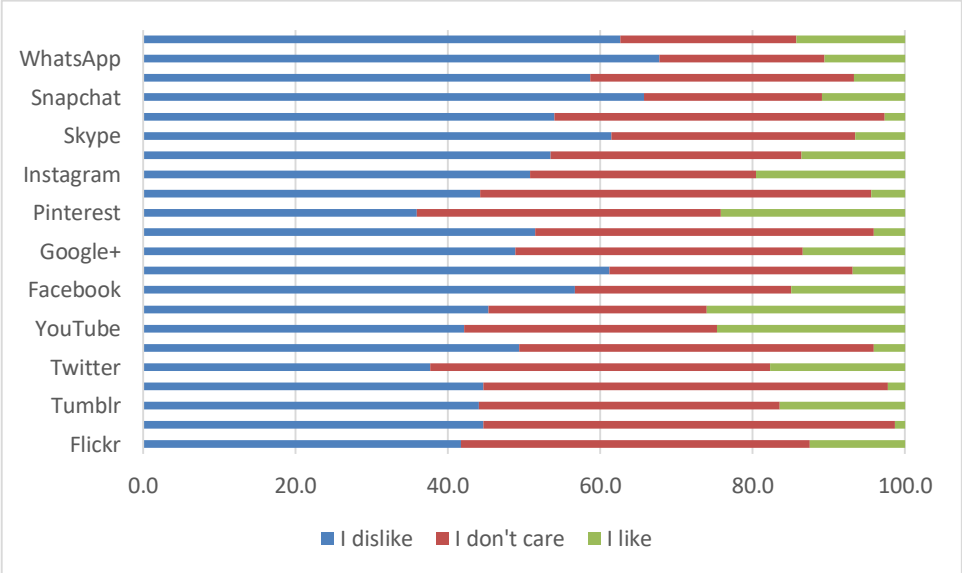

Figure 5. Assessment of personal data use according to user type. Share of respondents (users/non-users) that dislike/do not care/like that the respective online service uses their personal data, in percent. N=3,000

This acceptance of data collection and usage as long as the additional utility is perceivable, is also shown by Bitkom (2015). After all, almost half of the Internet users surveyed are more willing to provide their data the more useful the service is to them. Taddicken (2013) explains that users tend to share more personal information online the more they appreciate social networks. According to Chang and Heo (2014), the perceived benefit of using Facebook is correlated with the publication of personal information – but not with the perceived risks.

There are significant differences in the perception and assessment of the use of data (here: awareness), depending on whether the respondents use many of the services (i.e. are heavy users), depending on the gender and depending on whether or not they are high school students. For this sub-analysis, t-tests were performed on the equality of means of the respective subsamples of the surveyed students (see table 2). The interpretation of the values is mainly done via the sign and less via the value. If the sign is positive and the value is statistically significant, the respondents to whom the characteristic in the column applies (e.g. being a heavy user) are on average less aware than those to whom this characteristic does not apply. If the sign is negative and the value statistically significant, the respondents to whom the characteristic applies are more aware (e.g. identifying as female).

Table 2. Differences in privacy awareness. Results of t-tests on the equality of means of different subsamples with regard to privacy awareness; ***/**/* significance on the 1/5/10 percent level; a negative sign means that the subsample for which the respective characteristic is fulfilled is more aware of privacy issues than the subsample for which the characteristic is not fulfilled; a positive sign means that they are less aware

Subsample	Heavy User	Female	Secondary school (Gymnasium)	Of full age (>= 18 years old)	East Germany
Difference	0.0698**	-0.157***	-0.0421*	-0.0129	-0.0009
t-statistics	(3.26)	(-7.40)	(-2.34)	(-0.64)	(-0.08)

For the frequent users, data usage is less critical – which is why they seem to be more likely to use these services. Statistically significant differences also exist between the sexes: the male respondents are on average less critical than the female respondents. This confirms the results of a study among American university students (Peluchette / Karl, 2008).

In addition, respondents who go to the secondary school type “Gymnasium” are more critical than those who attend other types of schools that are less probable to be the basis for higher education. This is also seen in a US study: according to Rainie et al. (2013), people with a degree in higher education are more likely to use privacy measures such as clearing the browser history and cookies than people that are less educated. Also according to Blank et al. (2014), people with higher educational degrees rather change their privacy settings.

Statistically significant differences between students of full age (18 years old or older) and minors as well as between respondents from East and West Germany do not exist. The former is confirmed by Taddicken (2013), who sees a weak relationship between age and information sharing in social networks as well as privacy concerns for a German sample. Hoofnagle et al. (2010) support this finding for an American sample. They find no significant differences in privacy concerns between young adults and older adults. Blank et al. (2014), on the other hand, state that respondents in the age group 14 to 17 years particularly check their data protection settings, whereas older users do so much less frequently. Comparisons with other studies have the limitation that some of the samples show clear differences and thus are not very comparable.

2.4 Willingness to pay for Privacy

Although most students dislike that their personal data is stored and used by online social services, more than half of them are not willing to pay for services that do not use their data. The willingness to pay for privacy-friendly services is low. However, explicit surveys may lead respondents to cite extreme values rather than implicit surveys (Schwarz, 1999) or to give socially desirable or expected answers (Frik/Gaudeul, 2016). A hypothetical willingness to pay may differ greatly from the actual willingness to pay. Especially in a school context, the direct question about the assessment of data exploitation may trigger a "teacher-compliant" response. This indicates that the willingness to pay might be underestimated in this study.

A total of 55 percent of the respondents would not pay services such that these do not store and use their personal data (see table 3). 16 percent would spend less than 5 euros for privacy-friendly services, 3 percent even say they want to spend 30 euros and more.

Table 3. Willingness to pay for data protection; shares in percent, n=2,715

Amount per month in Euros	0 euro	0 to 5 euros	5 to 10 euros	10 to 30 euros	More than 30 euros
Share	55%	16%	12%	14%	3%

The willingness to pay increases only marginally with age. While the surveyed 14-year-olds were willing to spend an average of 3.80 euros, the average for students of full age (18 years or older) was 4.60 euros. This marks a small difference against the backdrop that older students can usually resort to more financial resources than younger ones. Measured against the upper limit of the pocket money recommended by the German Savings Banks Association (Deutscher Sparkassen- und Giroverband; see BMFSFJ, 2018), the willingness of 14-year-olds to pay for privacy amounts to 12.6 percent of their pocket money (30 euros pocket money). For the 15-year-olds it is 11.9 percent (37.50 euros pocket money), for the 16-year-olds 10.5 percent (45 euros), for the 17-year-olds 7.0 percent and for the students of full age 6.2 percent of their pocket money (75 euros). Relative to the average available pocket money, the willingness to pay thus decreases with age.

If one considers the mean values of different subsamples of the respondents, one finds that there is more of a positive willingness to pay (compared to one of zero), if the respondents are classified as "aware" due to their data protection preferences (see table 4). However, heavy users, i.e. respondents who use at least four of the considered services, are not significantly more often willing to pay than light users. This is related to the fact that heavy users, as shown in table 1, are rather less critical of the lack of data protection or the use of personal data and hence do not want to pay for better data protection.

There is a significant difference in the willingness to pay between female and male respondents: female students tend to be more often willing to pay for privacy than male students. They are also more critical (see table 1). Gymnasium students would pay more than other students. Whether a student is of full age (18 years and older) or not or whether he or she lives in East Germany or not, does not result in a significantly different willingness to pay.

Table 4. Differences in willingness to pay for privacy. Results of t-tests on the equality of means of different subsamples with regard to the willingness to pay for privacy (either 0 or positive); ***/**/* significance on the 1/5/10 percent level; a negative sign means that the subsample for which the respective characteristic is fulfilled is rather willing to pay for privacy than the subsample for which the characteristic is not fulfilled

Subsample	Aware	Heavy User	Female	Secondary school (Gymnasium)	Of full age (>= 18 years old)	East Germany
Difference	-0.110***	0.0537**	-0.0570**	-0.0531**	0.0176	0.0129
t-statistics	(-6.49)	(2.78)	(-2.96)	(-3.29)	(0.97)	(1.35)

Overall, the analysis shows that many students are critical of the storage and use of their personal data by online services. At the same time, the willingness to pay for more privacy-friendly services is low. Although 73 percent of the surveyed students value privacy ("are aware"), only 45 percent are willing to pay for it. Even among those who are "aware", only 49 percent are willing to pay for privacy. This result is even more striking if one considers that a polled, hypothetical willingness to pay is underestimated compared to the actual willingness to pay because it is not accompanied by actual costs (Benndorf/Normann, 2014).

2.5 Limitations

This analysis of privacy preferences by digital natives has several drawbacks that need to be taken into consideration. First, the term "digital natives" is misleading. It suggests that the surveyed students (aged 14 to 21 years old) have a high level of digital literacy, which does not need to be the case. By contrast, they might even choose to live very "offline". Digital natives in this context means that they grow up in an area that is per se very digital, as digitalization has advanced very much in the last two decades.

Second, the analyzed socio-economic factors are very limited. This is the case because the survey was conducted as final opinion survey of the JUNIOR program and not with a purely scientific orientation. It would be desirable to consider many more factors that might influence privacy preference, such as the level of education or the degree of digital literacy of the parents. It is assumed that there exists a certain path dependency that impacts the students' preferences. Also, the socioeconomic status including the household income could be relevant. It could be also interesting to link the dataset to other relevant datasets. A proper, econometric model based on behavioral economics would significantly enhance the study. Given the restrictions of the survey, this was not within the realms of possibility, but is certainly warranted further research.

3. CONCLUSION

This study confirms the privacy paradox for a sample of digital natives, 3,000 interviewees between the ages of 14 and 21, in Germany. Most respondents use online social services that store, process and exploit data on a broad basis, even though they are critical of data processing. Although many respondents know about privacy issues and show different privacy preferences depending on the social online service used, the majority is not willing to pay even only in theory for more privacy-friendly services. However, 45 percent of the students state that they want to pay at least a small amount for an increased level of data protection.

That digital natives completely dispense with online services because they disagree with their use of personal data, cannot be seen from the results either. Among the 14 percent who do not use any of the services, the share of those who are critical of lacking data protection is 65 percent, lower than the share among users (74 percent). Above all, the critical attitude of the users of communication services suggests that many students do not see any additional benefits which arise from the use of personal data, but they also rely on these services and hence continue to use them, nevertheless.

At this point, the previously discussed network effects play a crucial role: if the social environment of a student uses a privacy-friendly messenger, it is very probable that the user will also use a privacy-friendly messenger, even if she has to pay for it. In return, she will not use a more privacy-friendly messenger if her friends do not, because communication with them will then become more difficult and network effects cannot be skimmed off (see Engels/Grunewald, 2017).

The EU data protection regulation GDPR (see European Union, 2016) strengthens data protection. If companies process personal data, they must obtain explicit consent from their customers ("opt-in"). In particular, children and adolescents up to the age of 16 years may consent to the processing of their personal data for online services only with the consent of their parents. However, this age limit can be reduced by individual member states to 13 years (Article 8). Other parts of the regulation also explicitly protect children: data protection rules must be clear and understood when aimed at children (Recital 58) and measures such as profiling and automated decisions should not affect children (Recital 71). However, the verification of compliance with these requirements is difficult or even impossible.

It can be assumed that users will continue to release more personal data than they receive benefits in return. The question arises how incentives can be created to ensure that the existing need for data protection of the digital natives is taken into account by the social online services. At present, there are few incentives for companies to make their online services data protection-friendly because there is hardly any willingness to pay for such services. Laboratory studies could provide adequate experimental space for an array of different rules and regulations and thus determine what potential incentives could look like and how they can be enforced and guaranteed.

REFERENCES

Acquisti, A. and Gross, R., 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, in: Hutchison, K. et al. (eds.), Privacy Enhancing Technologies, Berlin, pp. 36–58

Acquisti, A. et al., 2015. Privacy and human behavior in the age of information, Science, Vol. 347, No. 6221, pp. 509–514

Acquisti, A. et al., 2016. The Economics of Privacy, Journal of Economic Literature, Vol. 52, No. 2, pp. 442–492

Barth, S. and de Jong, M., 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review, Telematics and Informatics, Vol. 34, No. 7, pp. 1038 – 1058

Benndorf, V. and Normann, H., 2014. The Willingness to Sell Personal Data, DICE Discussion Paper, No. 143, Düsseldorf

Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., 2015. Datenschutz in der digitalen Welt, https://www.bitkom.org/Presse/Presseinformation/Internetnutzer-gehen-pragmatisch-mit-Datenschutz-um.html [10-1-2018]

Bitkom, 2017. Nur jeder Fünfte hält seine Daten im Netz für sicher, https://www.bitkom.org/Presse/Presseinformation/Nur-jeder-Fuenfte-haelt-seine-Daten-im-Netz-fuer-sicher.html [1.2.2018]

Blank, G. et al., 2014. A New Privacy Paradox: Young people and privacy on social network sites, Annual Meeting of the American Sociological Association, San Francisco

BMFSFJ - Bundesministerium für Familie, Senioren, Frauen und Jugend, 2018. Taschengeld, http://www.familien-wegweiser.de/wegweiser/stichwortverzeichnis,did=38294.html [1-5-2018]

Chang, C. and Heo, J., 2014. Visiting theories that predict college students' self-disclosure on Facebook, Computers in Human Behavior, Vol. 30, pp.79 – 86

Engels, B., 2016. Data portability among online platforms, Internet Policy Review, Vol. 5, No. 2

Engels, B. and Grunewald, M., 2017. Das Privacy Paradox: Digitalisierung versus Privatsphäre, IW-Kurzbericht, No. 57, Köln

European Commission, 2015. Data Protection Report, Special Eurobarometer 431, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf [2-5-2018]

Evans, D. and Schmalensee, R., 2007. The Industrial Organization of Markets with Two-Sided Platforms, Competition Policy International, Vol. 3, No. 1, pp. 151 – 179

European Union, 2016, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Frik, A. and Gaudeul, A., 2016. The Relation between Privacy Protection and Risk Attitudes, with a New Experimental Method to Elicit the Implicit Monetary Value of Privacy, CEGE Discussion Papers, No. 296, Göttingen

Hann, I. et al., 2002. Online Information Privacy: Measuring the Cost-Benefit Trade-Off, ICIS 2002 Proceedings, http://aisel.aisnet.org/icis2002/1 [2.2.2018]

Hoofnagle, C. et al., 2010. How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?, https://repository.upenn.edu/cgi/viewcontent.cgi?article=1413&context=asc_papers [9.5.2018]

JUNIOR, 2018. Wirtschaft erleben – in einer JUNIOR Schülerfirma, https://www.junior-programme.de/

junior-schueler-erleben-wirtschaft/ [1-30-2018]

Keith, M. et al., 2013. Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus with Actual User Behavior, International Journal of Human-Computer Studies, Vol. 71, No. 12, pp. 1163–1173

Mpfs – Medienpädagogischer Forschungsverbund Südwest, 2018. JIM-Studie 2017, Jugend, Information, (Multi-)Media, Stuttgart

Li, T. and Unger, T., 2012. Willing to pay for quality personalization? Trade-off between quality and privacy, European Journal of Information Systems, Vol. 21, No. 6, pp.621 – 642

Nissenbaum, H., 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford

O'Donoghue, T. and Rabin, M., 2000. The Economics of Immediate Gratification, Journal of Behavioral Decision Making, Vol. 13, No. 2, pp. 233–250

Peluchette, J. and Karl, K., 2008. Social Networking Profiles: An Examination of Student Attitudes Regarding Use and Appropriateness of Content, CyberPsychology & Behavior, Vol. 11, No. 1, pp. 95 – 97

Pollack, L., 2016. What is the price for your personal digital dataset?, Financial Times, https://www.ft.com/content/1d5bd1d0-15f6-11e6-9d98-00386a18e39d [3-12-2018]

Rainie, L. et al., 2013. Anonymity, Privacy, and Security Online, http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/ [3-12-2018]

Schreiner, M. and Hess, T., 2015. Why Are Consumers Willing to Pay for Privacy? An Application of the Privacy-Freemium Model to Media Companies, Proceedings of the 23rd European Conference on Information Systems (ECIS), Münster

Schwarz, N., 1999. Self-Reports: How the Questions Shape the Answers, American Psychologist, Vol. 54, No. 2, pp. 93–105

Stiftung Neue Verantwortung, 2017. Datenpolitik jenseits von Datenschutz, Berlin

Sutanto, J. et al., 2013. Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users, Management Information Systems Quarterly, Vol. 37, No. 4, pp. 1141–1164

Taddicken, M., 2013, The "Privacy Paradox" in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure, Journal of Computer-Mediated Communication, Vol. 19, No. 2, pp. 248 – 273