PRIVACY CONCERNS IN MOBILE COMMUNICATION. A USER'S PERSPECTIVE

DELIA CRISTINA BALABAN*
MARIA MUSTĂȚEA*

Abstract The massive use of online platforms has contributed to an intensifying flow of collection, usage, and sharing of personal information of users. Technological development allows every form of user interaction to be transformed into data. The use of mobile devices on a large scale has added more dimensions to the online privacy debate. Within the theoretical framework of the protection motivation theory (PMT), our study aimed to analyse the privacy protection behaviour related to mobile communication. The motivation of individuals to protect themselves from threats depends on two aspects: a threat assessment and a coping assessment. We conducted eight group interviews with N=92 German early-stage adults regarding data privacy concerns and coping strategies. The conclusions drawn from our study are that respondents clearly showed a preoccupation with their mobile data protection, but they do not consider information protection in mobile communication as much of a choice. Users are aware that they have certain safety leverages to use in order to protect their data, but they are far more limited than those applied to online communication using computers. Technology is not necessarily friendly to information protective behaviour. Users identified some limited response efficacy measures to take so as to protect their privacy when it comes to app settings.
Keywords Data privacy, data protection, social networks, data disclosure, privacy management.

* *Babeș-Bolyai University, Cluj-Napoca*. balaban@fspac.ro.
* *Babeș-Bolyai University, Cluj-Napoca*. mustatea@fspac.ro.
DOI: 10.26424/philobib.2021.26.1.06

With the development of data-mining technologies, online data protection has come under the focus of both scholars and public opinion.[1] The massive use of online platforms has contributed to an intensifying flow of collection, usage, and sharing of the users' personal information. Technological development allows every form of user interaction to be transformed into data. Data is a valuable resource for companies that systematically collect and analyse users' information. This type of practice has raised concerns among platform users.[2] The complexity of privacy challenges is associated with the complexity of technological development.[3] There are two approaches when it comes to protecting users' online information: educating individuals, so they become responsible for their privacy, and moving the responsibility to the authorities. They should impose protection through executive, legislative and judicative actions.[4]

Users are most concerned about the access to or distribution of their personal information by unauthorized parties, which could result in potential harm to their safety. They are also aware of the fact that privacy settings are vulnerable, thus preferring to rely on their instincts to prevent possible leaks, even though privacy settings are difficult to fully grasp most of the time.[5]

For better protection of its citizens, the European Union countries introduced the *ePrivacy Directive* in 2009 and the EU *General Data Protection Regulation* (GDPR) in 2016. According to EU regulations, the collection of data is permitted only with the users' consent.[6] Even so, the regulations do not fully cover the modern data processing practices that are constantly evolving.

There are benefits to disclosing information online for both users and companies,

[1] Jan Fernback, Zizi Papacharissi, "Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies," *New Media & Society* 9 (5), 2007: 715-34. doi:10.1177/1461444807080336.

[2] Jose van Dijck, Thomas Poell, Martijn De Wall, *The platform society. Public values in a connective world* (Oxford University Press: 2018)

[3] Christoph Lutz, Maren Schöttler, Christian Peter Hoffman, "The privacy implications of social robots: Scoping review and expert interviews," *Mobile Media & Communication* 7 (3), 2009: 412-434. doi:10.1177/2050157919843961.

[4] Thilo von Pape, Sabine Trepte, Cornelia Mothes, "Privacy by disaster? Press coverage of privacy and digital technology," *European Journal of Communication*, 1-19 (2017). doi:10.1177/0267323117689994.

[5] Deirdre McGuinness, Anoush Simon, "Information disclosure, privacy behaviours, and attitudes regarding employer surveillance of social networking sites," *International Federation of Library Associations and Institutions* 44 (3), 2018: 203-222.

[6] Kathrin Bednar, Sarah Spiekermann, Marc Langheinrich, "Engineering Privacy by Design: Are engineers ready to live up to the challenge?" *The Information Society*, 1-22 (2019). doi:10.1080/01972243.2019.1583296.

such as building better social connections, improving website usability, personalizing the messages the latter promote, convenience, and efficiency. Within the paradigm of "user empowerment," the role of self-management of personal information is becoming more important. Information literacy, which includes the technical architecture of the internet, the awareness of common practices and policies, allows users to take an "informed control of their digital personalities.[7]"

The use of mobile devices on a large scale has added more layers to the online privacy debate. Users of mobile devices have expressed concerns that by using certain apps private information may be shared with third-party delivery services, marketers and analytic companies. Location tracking technologies that share information to third parties without the users' consent are also subject to criticism.[8] In this context, the present research aims to address the issue of users' privacy concerns and their coping strategies when using mobile communication.

Defining privacy

Privacy has been defined as the "temporary withdrawal of a person from the general society through physical and psychological means.[9]" Privacy is a legal concern tied to individual and collective rights, expressed through social interactions. It is the "claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others.[10]" Privacy has dynamic components that make a difference between various types of theories, such as access theories, control theories, and restricted access/ limited control theories. Control theories offer an overview of self-determination over privacy, and restricted access ones conceive privacy as a moral structure meant to protect humans.[11] From an individual's point of view, *privacy* is the correspondent of the *private sphere*- a situation, a room or space. Based on various settings, people wish to have a certain level of privacy which represents their ideal level of interaction with others.[12]

[7] David Barnard-Wills, Ashenden Debi, "Playing with Privacy: Games for Education and Communication in the Politics of Online Privacy," *Political Studies* 63 (2015), 143. doi:10.1111/1467-9248.12049.

[8] Janice C. Sipior, Burke T. Ward, Linda Volonino, "Privacy Concerns Associated with Smartphone Use," *Journal of Internet Commerce* 13 (1), 2014: 177-193. doi:10.1080/15332861.2014.947902.

[9] Alan F. Westin, *Privacy and freedom* (New York, NY: Atheneum, 1967), 7.

[10] Alan F. Westin, "Privacy and freedom," *Social Work* 13 (4), 1968: 6-7.

[11] Stylianos Papathanassopoulos, "Privacy 2.0," *Social Media + Society* (April-June 2015), 1-2. doi:10.1177/2056305115578141.

[12] Philipp K. Masur, Michael Scharkow, "Disclosure Management on Social Network Sites: Individual Privacy Perceptions and User-Directed Privacy Strategies," *Social Media + Society* (January-Ma 2016), 1-13. doi:10.1177/2056305116634368.

Burgoon (1982) identified four dimensions of privacy. The first one is the *informational* dimension, which refers to the control over personal information. The second one is *the social* dimension that reveals the distance to the others. The *physical* dimension is defined by allowing access to someone's premises or body. And finally, the *psychological* dimension includes intimacy and the depth of exchange with others.[13] Three out of four dimensions apply to online privacy, the only one which does not, is the physical dimension.[14]

The concept of *privacy concerns* looks at individuals' beliefs about possible negative consequences that are associated with information disclosure and sharing. Among the most frequent measures to protect online privacy, users mentioned removing one's information from commercial databases, deleting the cookies and avoiding self-disclosure.[15]

Information disclosure

Previous literature has suggested that the association between social media and privacy is problematic to a certain extent. Social networking sites continue to serve as global venues for personal disclosure. Depending on the privacy settings and on the social network site that people choose, information disclosure is not only made to close friends and family but also to a larger audience. Social media platforms offer the means to communicate to large and diverse networks of people. This is fuelled by peer pressure, the desire to be portrayed in a certain manner, the trust in the network, and the perceived benefits vs. costs of information sharing. The users wish to identify with the online communities and affirm their membership among other users. Individuals may manage their online privacy by controlling the amount of information they upload or control access through privacy settings.[16]

[13] Judee K. Burgoon, "Privacy and communication," *Annals of the International Communication Association* 6 (1), 1982: 206-249. doi:10.1080/23808985.1982.11678499.

[14] Nicole C. Krämer, Nina Haferkamp, "Online Self-Presentation: Balancing Privacy Concerns and Impression Construction on Social Networking Sites," in *Privacy Online*, eds. S. Trepte, L. Reinecke (Heidelberg: Springer, 2011), 127-141; Yannic Meier, Johanna Schäwel, "No risk – no fun. The Role of Risk-Attitudes and the Need for Cognition in Online Privacy Decision-Making," in *Conference Paper. International Communication Association (ICA)* (Washington, DC: 2019), 1-33.

[15] Lemi Baruh, Ekin Secinti, Zeynep Cemalcilar, "Online Privacy Concerns and Privacy Management: A Meta-Analytical Review," *Journal of Communication* 67 (2017): 26-53.

[16] McGuinness, Simon, "Information disclosure, privacy behaviours, and attitudes regarding employer surveillance of social networking sites"…, 203-22.

Privacy and mobile communication

In recent years, users have seen a large diversification of media platforms and increased accessibility of social networking sites on mobile devices. This has allowed for an increased exchange of data in the virtual climate.[17] In the context of mobile communication, the discussion about information disclosure and privacy has reached a new level of complexity.[18] Most of these platforms are accessed now via applications on mobile devices, where a consistent amount of identifiable information is aggregated, archived and linked across multiple platforms.[19] One of the privacy concerns expressed regarding mobile communication is that by using smartphones, tablets, etc. information could be shared with third-party delivery services, marketers, and analytics companies with the help of apps and of location tracking technologies. Added to this, the devices have subscriber identity modules and other identification mechanisms. The former facilitates data collection and sharing among several entities. This is associated with privacy concerns which include mobile malware, information collection by smartphone, network and app providers regarding location and movements, as well as loss and / or theft.[20] Online protection behaviour is a specific computer-based action that users take to protect their information.[21] Similar to the definition mentioned above, protection behaviour related to mobile communication can be defined as a specific communication-based action performed on mobile devices to protect their information.

Theoretical approaches to online privacy

The privacy paradox model, which states that users share a vast amount of online information and are simultaneously concerned about online privacy, is one of the theoretical perspectives. The privacy paradox is related to a so-called privacy

[17] Mina Tsay-Vogel, James Shanahan, Nancy Signorielli, "Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users," *New Media & Society* 20 (1), 2018: 141-61. doi:10.1177/1461444816660731.

[18] Sabrina Karwatzki, Olga Dytynko, Manuel Trenz, Daniel Veit, "Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization," *Journal of Management Information Systems* 34 (2), 2017: 369-400. doi:10.1080/07421222.2017.1334467.

[19] Hsuan-Ting Chen, "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), 2018: 1392-1412. doi:10.1177/0002764218792691.

[20] Sipior, Ward, Volonino, "Privacy Concerns Associated with Smartphone Use"…, 177-93.

[21] George R. Milne, Lauren I. Labrecque, Cory Cromer, "Toward an understanding of the online consumer's risky behavior and protection practices. Journal of Consumer Affairs," *The Journal of Consumer Affairs* 43 (3), 2009: 449-473. doi:10.1111/j.1745-6606.2009.01148.x.

apathy.[22] This phenomenon was observed concerning the use of social network sites where a large quantity of information was shared, people had the illusion of privacy and a discrepancy between context and behaviour was observed. Users had low knowledge about what can happen with their data.[23]

Social network sites have developed in the last years and so, users can consider privacy when configuring their settings. These enable them to choose with whom they share specific types of content. In the aftermath of scandals such as Cambridge Analytica, Facebook responded to public criticism and has given more attention to privacy details since 2017. There is also an ongoing process of diversification of social network platforms that serve different purposes: Snapchat is designed for ephemeral communication, Instagram or Twitter are promoted as "tools for public expression," WhatsApp encourages communication inside groups.[24] Recent studies have suggested there are not so many differences between the stated intentions and the actual behaviour regarding online privacy.[25] People have a certain amount of confidence in some protective measures but have little confidence in their efficacy in protecting their online privacy.[26]

The privacy calculus model indicates that people decide how much they want to disclose about themselves, based on the balance between the benefits they believe they get and the perceived costs. Users make rational decisions concerning how to protect their privacy.[27] When such advantages outweigh the costs, people will be more inclined to disclose data. The disclosure on social network sites is determined by experience and by the benefits that are perceived to be higher than

[22] Eszter Hargittai, Alice Marwick, "What can I really do? Explaining the privacy paradox with online apathy," *International Journal of Communication* 10 (2016): 3737-57.

[23] Susan B. Barnes, "A privacy paradox: Social networking in the United States. First Monday," *First Monday* 11 (9), 2006. doi:10.5210/fm.v11i9.1394; Alessandro Acquisti, Ralph Gross, "Imagined communities: Awareness, information sharing, and privacy on the Facebook," in *Proceedings of 6th Workshop on Privacy Enhancing Technologies*, eds. P. Golle, G. Danezis (Cambridge: Robinson College, 2006), 36-58; Tobias Dienlin, Sabine Trepte, "Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors," *European Journal for Social Psycology* 45 (3), 2015: 285-97. doi:10.1002/ejsp.2049.

[24] Trottier, Daniel, "Privacy and Surveillance," in *The SAGE Handbook of Social Media* (Sage Publications Ltd, 2017), 463-78.

[25] Baruh, Secinti, Cemalcilar, "Online Privacy Concerns and Privacy Management: A Meta-Analytical Review"…, 26-53.

[26] Sophie C. Boerman, Sanne Kruikemeier, Frederik J. Zuiderveen Borgesius, "Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data," *Communication Research* 00 (0), 2018: 1-25. doi:10.1177/0093650218800915.

[27] Mary J. Culnan, Robert J. Bies, "Consumer privacy: Balancing economic and justice considerations," *Journal of Social Issues* 59 (2), 2003: 323-42. doi:10.1111/1540-4560.00067.

the risk.[28] Further research has underlined the idea that self-disclosure on social media and self-withdrawal are not mirrored images, but two distinctive behaviours on social network sites. Disclosure and withdrawal stand in a dialectic relationship and users establish rules for both.[29]

Disclosing information has perceived benefits. People are tempted to share information, as it facilitates their recognition as valid members of a community, brings status,[30] contributes to social capital.[31] In terms of risk, disclosing information can sometimes lead to interpersonal boundary turbulences, which could bring about negative consequences in offline interactions. Privacy concerns are influenced by age, as older people express concerns more often than younger people.[32] Western countries are preoccupied with the issue of diffusion and appropriation of data.

The theoretical models presented above argue that the cost-benefit analysis is rationally based. Other models argue that people cannot always make rational decisions due to bounded rationality, which refers to the fact that decision-makers are inevitably constrained by limited information, limited capacity to process information, and limited time.[33] Users make online privacy decisions based on cognitive heuristics that may bias the way they perceive risk.[34] Cognitive heuristics are mental shortcuts; rules of thumb that users seem to employ when

[28] H. Krasnova, S. Spiekermann, K. Koroleva, T. Hildebrand, "Online social networks: Why we disclose." *Journal of Information Technology* 25 (2), 2010: 109-25. doi:10.1057/jit.2010.6; Hanna Krasnova, Natasha F. Veltri, Oliver Günther, "Self-disclosure and privacy calculus on social networking sites: e-role of culture," *Business & Information Systems Engineering* 4 (3), 2012: 127-35. doi:10.1007/s12599-012-0216-6.

[29] Tobias Dienlin, Miriam J Metzger, "An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample," *Journal of Computer-Mediated Communication* 21 (5), 2016: 368-83. doi:10.1111/jcc4.12163.

[30] David Barnard-Wills, Ashenden Debi, "Playing with Privacy: Games for Education and Communication in the Politics of Online Privacy," *Political Studies* 63 (2015): 142-60. doi:10.1111/1467-9248.12049.

[31] Sinon Gonen, Noa Aharony, "Relations between Privacy Behaviors and Social Capital on Facebook," *International Journal of Libraries and Information Studies* 67 (2), 2017: 103-18. doi:10.1515/libri-2016-0096.

[32] Priscilla M. Regan, Gerald FitzGerald, Peter Balint, "Generational views of information privacy?" *Innovation: The European Journal of Social Science Research* 26 (1-2), 2013: 81-99. doi:10.1080/13511610.2013.747650.

[33] Herbert A. Simon, 1997. "Bounded rationality. In Models of bounded rationality: Empirically grounded economic reason (Vol. 3, pp. 291–294). Cambridge, MA: The MIT Press," in *vol 3* (Cambridge MA: The MIT Press, 1997), 291-94.

[34] Acquisti, Gross, "Imagined communities: Awareness, information sharing, and privacy on the Facebook"…, 36-58.

disclosing or withdrawing information.[35]

Previous research on the use of heuristics in privacy protection behaviour identified positive heuristics that increased information disclosure behaviour and negative heuristics that inhibited information disclosure in several privacy-related online contexts such as the use of mobile communication, e-commerce, and cloud services. Gambino et al. (2016) identified positive heuristics such as: gatekeeper heuristic (a system which has several layers of access is perceived as safe), safety net heuristic (in terms of safety, a third party is covering for me), bubble heuristic (the safety of a protected network, such as one's own Wi-Fi), and ephemerality heuristic (platforms that show the disclosed information only for a short period of time are perceived as safer). The identified negative heuristics were: fuzzy-boundary heuristic (information may be shared with third-parties), intrusiveness heuristic (unsolicited requests are perceived as unsafe), uncertainty heuristic (a difficult to understand interface is perceived as unsafe), and mobility heuristic (mobile communication gadgets are perceived as unsafe).[36]

Users provide rationales for their online privacy behaviour when it comes to the use of social network sites such as Facebook. Suh & Metzger[37] identified a set of heuristics that applied to privacy concerns when disclosing information on social network sites: affect heuristic (emotions can influence users' judgment on the risk perception of information disclosure), availability heuristics (negative experience become more salient), bubble heuristics (the use of one's own Wi-Fi connection, private mode), homophily heuristic (feeling safe to disclose information with peers), bandwagon heuristic (users' tendency to go along with the crowd), inequality aversion (companies that use data without paying the users anything for it), hyperbolic disclosing (users tend to perceive short term risks as being higher than long term risks) and ephemerality heuristic (users trust formats where their information is visible only for a short time).[38]

The communication privacy management theory suggests people believe they have the right to control their private information and decide who is allowed to

[35] Amos Tversky, Daniel Kahneman, "Judgment under uncertainty: Heuristics and biases. Science," *Science* 185 (4157), 1974: 1124-31. doi:10.1126/science.185.4157.1124.

[36] Andrew Gambino, Jinyoung Kim, S. Shyam Sundar, Jun Ge, Mary Beth Rosson. 2016. "User disbelief in privacy paradox: Heuristics that determine disclosure," in *Conference on Human Factors in Computing Systems - Proceedings*, 07-12-May (San Jose CA., 2016), 2837-43. doi:10.1145/2851581.2892413.

[37] Jennifer Jiyoung Suh, Miriam Metzger, "Privacy Decision-Making on Social Network Sites: The Role of Heuristics," in *Conference Paper. International Communication Association (ICA)* (Washington D C, 2019), 1-37.

[38] Ibid.

access it.[39] The theory has contributed to the understanding of privacy issues in computer-mediated communication.[40] It addresses the relationship between disclosure and privacy, examining how and why people decide to reveal private information or not.[41] Disclosure has benefits and risks, with individuals putting the two in the balance. Among the benefits of information disclosure, previous research has identified self-expression and relationship development and, among the risks, loss of status, reputation and control are mentioned. When people disclose, they give something away, in the form of shared information, but they still want to feel like they are the ones who retain control. To this end, individuals develop rules to aid their decisions of disclosure.[42]

The protection motivation theory adds the component of individual efficacy to the previous models. Instead of focusing on the reasons why people do not disclose information, it provides a framework for understanding if people perceive any possible threats and if they believe they are capable of countering them. The individuals' motivation to protect themselves from threats depends on two aspects: a threat assessment and a coping assessment. The threat assessment implies the perceived severity and the perceived susceptibility, while the coping assessment looks at self-efficacy and response efficacy. Self-efficacy is defined as the belief in one's ability to perform a certain behaviour and response efficacy includes the tools to perform it.[43] People have little confidence they can protect their information online, yet they believe some responses can effectively eliminate the collection and usage of their data. This lack of knowledge seems to be reflected in the people's perception of their ability to secure their online privacy.[44]

Within the theoretical framework of the protection motivation theory, our study aimed to analyse the privacy protection behaviour related to mobile communication. In order to gain insight into the threat assessment and coping assessment dimensions we asked the following research questions:

RQ1. What are the privacy concerns and how do users evaluate privacy threats related to mobile communication?

---

[39] Sandra Petronio, *Boundaries of privacy: dialectics of disclosure*. *SUNY Press* (Albany, NY: State University of New York Press, 2002), doi:10.5860/choice.40-4304; Boerman, Kruikemeier, Zuiderveen Borgesius, "Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data"…

[40] Masur, Scharkow, "Disclosure Management on Social Network Sites: Individual Privacy Perceptions and User-Directed Privacy Strategies"…

[41] Miriam J. Metzger, "Communication Privacy Management in Electronic Commerce," *Journal of Computer-Mediated Communication* 12 (2007): 335-61.

[42] Ibid.

[43] Boerman, Kruikemeier, Zuiderveen Borgesius, "Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data"…, 1-25.

[44] Ibid.

RQ2. What are the coping strategies of mobile communication users when dealing with privacy threats and how efficient do users think they are?

Methodology

The empirical part of our study included eight group interviews with N=92 German early-stage adults regarding data privacy concerns and coping strategies. The age range was 19-25, and the groups were mixed-gender. The majority of the participants were students. We carried out eight group discussions in Germany in the time frame April-September 2019. There were 10-12 respondents in each focus group. They were all mixed-gender focus groups and each group discussion lasted no longer than 80 minutes. The main condition for voluntary participation in these focus groups was to be a smartphone user.

Data analysis was performed, based on categories related to the themes.[45] The main topics discussed were in line with our research questions: threat assessment and coping assessments in the protection of information privacy in mobile communication and the efficiency of the implementation of the GDPR. Participants were asked about their privacy concerns related to mobile communication and what measures they take to protect their information.

Results

Privacy concerns about mobile communication

Privacy, in general, is a very sensitive and important aspect for the respondents: “It is extremely important. If I have all my data shown online, anyone can stalk me and follow my every step” (22-year-old male). Privacy concerns are not only reduced to social media even if this is a field where one can have the perception of being able to control one’s privacy but "it is about everything, about *Alexa, Siri,* paying by credit cards and using several apps daily." (22-year-old female). Receiving so-called tailored advertising is a reason to be concerned: “it is unpleasant to be tracked online. Your search for an item, then you are targeted by ads for similar products, which gives you the feeling of being pressured into buying something” (22-year-old male). This phenomenon has reached a new height, as several users described: “sometimes when I am with my friends and we are discussing something, I receive ads on Facebook and not only on Facebook about that particular product. One day I was visiting a friend that has a cat and then for the next few days, I received several ads for cat food even if I don’t have a cat and have never had one. Besides, I have never

[45] John W. Creswell, *Research design- qualitative, quantitative and mixed method approaches* (Thousand Oaks, CA: Sage Publications, 2009).

searched for cat food online. It is as if our phones are recording what we are talking about and send us ads related to our conversations" (23-year-old female). Tailored ads are not perceived as negative by all participants: "I like the idea of receiving relevant advertising. Since we have no other choice but to see ads online, it would be good if they were customized" (23-year-old male).

The old ways of protecting online privacy that applied to computers are no longer efficient: "the cookies and the privacy settings you set cannot protect you" (21-year-old male). The lack of transparency of companies that collect data was underlined: "We are like open books for companies. They can read our behaviour. Some of them, like Facebook in a recent ad, claims to protect our collected data, but this is only an image strategy" (24-year-old female).

When it came to the use of smartphones, the interviewees expressed concerns their data is collected through the use of apps and sent to third parties: "you don't know what they do with your data" (25-year-old male) and that users have the right to know what is happening with their data: "I believe it is important to know who has access to and looks at your data" (22-year-old female). Thanks to data tracking technologies that are incorporated in smartphone apps, providers can "take info such as our name, our birthday, hobbies, but also places we have been to" (21-year-old female). "They take a lot of our data and use it for various purposes that we cannot imagine" (24-year-old male).

Even though they were aware of the fact that information was collected by several apps they used, some respondents underlined the idea that they did not know what kind of personal information the apps were collecting. There are some types of information that one can decide to share or not, such as name, address, email address, phone number, the Facebook or Google account that allows you to connect to the apps. But there is another type of information that users are unaware that it can be collected and shared with third parties. This is a phenomenon that cannot be controlled by users or there are only a few things that can be done to protect users: "it is almost impossible to live without a smartphone nowadays. Once you accept this, you understand that you have to think about how you use it and what you share" (21-year-old male).

The perceived threat assessment is not so high because of the lack of transparency of the data collecting companies: "if we could only see where our data is going, we would literally panic, but we do not have this ability" (21-year-old female) and because users did not pay much attention to data collection practices when smartphones were first introduced: "now it is too late. We should have been vigilant years ago" (24-year-old female).

Coping strategies to deal with privacy concerns in mobile communication

One of the main ideas when it comes to measures to protect data privacy in mobile communication is to read the terms and conditions carefully when downloading a new app or when updating one. The users we talked to were aware of the importance of taking this measure, but they admit they never do so because: "I don't have time to read the terms and conditions. Maybe I am too lazy, or maybe I don't do it because nobody reads them. Besides, they are presented in a very user-unfriendly way. Something must be done to make companies come up with a short, user-friendly version" (23-year-old female). The next element of privacy protection behaviour related to the use of apps is to carefully analyse the requests of the app, like permission to access one's microphone, camera, contact, location, and photo gallery: "it makes sense to permit access to your camera and photo gallery for a photo-processing app, but it makes no sense to allow this app access to your contacts or even to your location" (25-year-old female). It does not stop with the initial answer to the app's request, because from time to time "the app will ask for your permission, again and again, so you have to be careful all the time" (22-year-old male). There is a wide variety of apps, some of which are not necessary, so as a protective measure, users are invited to reflect on the necessity of downloading the app in the first place or on deleting an app if it proved to be too intrusive.

The idea of data as goods was emphasized. Within the logic of *datafication*[46] some of the users underlined the idea that data is collected by companies and this is and will be common practice: "we have to think about the idea that nothing is for free. We have access to services that we do not pay for with money, but with our data" (25-year-old male). The willingness to trade one's data was often expressed during our group discussions: "everything comes at a price. The use of our data is the price we pay to have an easier life, to have access to mobile technology" (24-year-old female).

As a protective behaviour, using an email address and not a Facebook or Google account for online interactions that are evaluated by users as unsafe is a strategy that is also applied to mobile communication. Mobile devices such as smartphones make certain activities much easier. The use of mobile devices is often associated with comfort. Using Facebook or Google accounts to register for an app is a matter of comfort as well: "to logon using Facebook is easy and sometimes we prefer the easiest way, without thinking too much about possible consequences for our privacy" (24-year-old female).

Some of the disclosed information is much more sensitive, such as information about health or finances: "it is dangerous when you think about the fact that you have access to your online bank accounts from your phone. You can easily

[46] Van Dijck, Poell, De Wall, *The platform society. Public values in a connective world…*

be a victim" (22-year-old female). The coping strategies are different in this situation: on the one hand, some respondents use home computers to do online banking and, on the other hand, others trust mobile banking apps, underlining the idea that these kinds of institutions cannot afford not to be safe. In addition to that, a new EU directive requires banks to implement additional safety measures for mobile banking. In the particular situation of the privacy of financial data, the biggest concerns are related to hacking, phishing and other criminal strategies that existed before the widespread use of smartphones.

To deal with this situation of low self-efficacy and low response efficacy some of our respondents stressed that they had nothing to hide. Nevertheless, the overall attitude suggested resignation in front of changes and the online phenomenon: "I think we cannot control what platforms use and what they do not" (25-year-old female). They do not perceive their information as being of interest to bigger parties: "our data is not so important. We are ordinary people. But in the case of important people or celebrities, there the risk is very high" (24-year-old male). There are different levels of efficiency ranging from: "you have a fake choice to protect your information" (24-year-old female) to "as individuals we have different levels of transparency, you can try to give them a minimum of transparency" (21-year-old female).

The perceived efficiency of the regulations concerning data privacy

In terms of protection, the respondents had mixed opinions about the newly-implemented GDPR: "on the one hand, it is good to have regulations like GDPR to protect your data. On the other hand, when they ask for approval for everything, it is absurd" (19-year-old male).

Others suggested that regulations such as GDPR were pointless in the bigger context: "sometimes it is useless. For instance, asking workers for consent for everything at work. When you got hired there, you became part of that company" (21-year-old male). Some even mentioned the aspect of public spaces where one should accept the fact that he/she is exposed: "if it is a public space, I think it is useless to ask for consent. If I was there, it was my choice. I deliberately chose to be seen" (21-year-old male), "GDPR is additional work, especially for small companies that have to ask permission for everything" (24-year-old male). The solution lies in "a constant monitoring process of big data collecting companies" (22-year-old male).

Conclusions

The first insight gained from our study is that respondents clearly showed a preoccupation with their mobile data protection. Nevertheless, they do not consider information protection in mobile communication as much of a choice. Technology is

not necessarily friendly to information protective behaviour.

The second relevant finding is that users identified some limited response efficacy measures to take to protect their privacy when it comes to app settings. In some situations, *take it or leave it* applies. If one does not accept the terms and conditions of an app, then it is impossible to use that app. People are aware that they have certain safety tools to use to protect their data, but they are far more limited than those applied to online communication using computers. Our findings are in line with previous research: when it comes to sensitive information, using computers or even avoiding online communication is still an option, but not for long.[47] People cope by changing their privacy settings on their accounts and deleting cookies, or by refusing to provide certain information or access to the camera, contact, microphone, and photo gallery when not necessary.

Third, users perceived data as a commodity that one could trade or give in exchange for using apps. Some of them underlined the idea that they are already paying through their collected data, others are even willing to give up the privacy of their data to companies in exchange for payment. This is a practice they consider to be fair as opposed to various companies' current common practices of collecting and sharing users' data.

The fourth finding is related to the idea that users think that states should regulate companies in this field much more efficiently than they are doing now within the framework of GDPR in EU countries.

The present research has an exploratory nature. We reveal aspects of data protection perceptions and behaviour of educated early-stage adults. Privacy concerns vary over time.[48] Previous literature on privacy revealed the importance of age and education when it comes to threat assessment and coping assessment.[49] As the cultural background is also important, German society stands out as it has an especially high degree of sensitivity.[50] Since we conducted group interviews and due to the nature of our sample, our findings cannot be generalized.

[47] Gambino et al, "User disbelief in privacy paradox: Heuristics that determine disclosure"…; Sipior, Ward, Volonino, "Privacy Concerns Associated with Smartphone Use"…

[48] See Sipior, Ward, Volonino, "Privacy Concerns Associated with Smartphone Use"…

[49] See Boerman, Kruikemeier, Zuiderveen Borgesius, "Exploring Motivations for Online Privacy Protection Behavior…"

[50] See von Pape, Trepte, Mothes, "Privacy by disaster? Press coverage of privacy and digital technology"…