Periods in the Public Eye: Investigating Risk Perceptions of Data Sharing in Reproductive Health Applications

Deubel, Annika; Heger, Pauline

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Deubel, A., & Heger, P. (2023). Periods in the Public Eye: Investigating Risk Perceptions of Data Sharing in Reproductive Health Applications. *easy_social_sciences*, 69, 37-44. https://doi.org/10.15464/easy.2023.11

easy_social_sciences 69 ▪ 2023

doi: 10.15464/easy.2023.11

Periods in the Public Eye

Investigating Risk Perceptions of Data Sharing in Reproductive Health Applications

Annika Deubel & Pauline Heger

Period tracking apps allow for tracking and monitoring various aspects of reproductive health, making them a convenient and popular choice for personal tracking. However, concerns have been raised regarding the data-sharing practices of such apps. Against this background, the study at hand investigated the perceived privacy risks of period trackers and connection to knowledge about data sharing practices among German users. Exploratory analyses reveal that users who actively use period trackers have a lower risk perception than those who have discontinued the use. Additionally, perceived knowledge of data sharing practices of period trackers shows a negative relation with risk perception.

Perioden-Tracking-Apps sind für viele Menschen ein beliebtes Mittel für die Überwachung verschiedener Aspekte der reproduktiven Gesundheit. Gleichzeitig gibt es jedoch zahlreiche Bedenken hinsichtlich der Datenweitergabepraktiken solcher Apps. Die vorliegende Studie untersucht die wahrgenommenen Datenschutzrisiken von Perioden-Trackern sowie die Rolle von Wissen über Datenweitergabepraktiken unter deutschen Nutzenden. Die explorativen Analysen zeigen, dass Nutzende, die Perioden-Tracker aktiv verwenden, eine geringere Risikowahrnehmung haben als solche, die die Verwendung eingestellt haben. Darüber hinaus steht das wahrgenommene domänenspezifische Wissen über den Umgang mit Daten von Perioden-Trackern in einem negativen Zusammenhang mit der Risikowahrnehmung.

Keywords: perceived privacy risk, mobile health, period trackers

The accelerated global diffusion of information and communications technology (ICT) has led to a significant increase in the use of mHealth, i.e., the use of mobile apps for healthcare. While such applications can be useful for many purposes and users, at the same time, the discussion surrounding the sharing of healthcare data has been a prevalent issue in recent years (Schnall et al., 2015; Schroeder et al., 2022). The recent significant changes in the legislation regulating abortions in the United States intensified these discussions. The loss of federal protection for abortion rights by the Supreme Court's decision to overturn Roe v. Wade in the US has sparked serious data privacy concerns over the abuse of medical records as well as information generated from a person's online activity worldwide (Somberg, 2022). One main concern is that reproductive health information collected by such apps may be used to infer whether someone is seeking an abortion. Even prior to this, concerns have been voiced worldwide about the quantity of data and metadata gathered and traded to third parties by most reproductive health apps (Alfawzan et al.,

2022). How perceptions of privacy risks may have changed in particular after the legislative changes regarding abortions within the US is, however, still unclear.

In the study we present in this article, we investigated how users perceive the privacy risks associated with data sharing via period trackers, particularly in light of these recent political developments. We especially look at the role of knowledge about data privacy and usage patterns regarding other mHealth apps, on the condition of being active users or having used period trackers in the past.

mHealth Usage and Period Trackers

Mobile Health (mHealth) refers to the use of mobile-enabled applications for collecting and providing health care information (Azhar & Dhillon, 2018). These applications offer the potential for users to continuously monitor and promote their health and well-being, detect issues early, or have an improved access to healthcare (Papageorgiou et al., 2018). One type of mHealth applications are period tracking apps, which have become increasingly popular over the years. As a subgroup of mHealth applications, they allow users to track and analyse their menstrual cycles and other related factors, such as birth control (Levy & Romo-Avilés, 2019). At present, over 200 million individuals worldwide are estimated to use period trackers (Healy, 2021).

To investigate the use of period tracking apps and associated perceptions of privacy risks, we conducted an online survey among individuals who are or have been using such apps. A total of 146 participants took part in the survey which was fielded between November 28th and December 19th, 2022. Regarding general usage, 82.2% of participants (i.e., 120 individuals) stated that they actively used period trackers at the time of their response. Figure 1 shows the reasons why active users are currently using a period tracker. Out of these, the majority (93.3%) use the app for tracking their menstrual cycle, while over half of them (58.3%) also want to better understand their cycle. Other reasons were predicting premenstrual syndrome (PMS), symptoms of endometriosis or using the app to have better control over their fertility. 17.8% (i.e., 26 participants) in our sample have used period trackers in the past but have stopped to do so. Figure 2 displays the reasons for discontinuing the use of period trackers. 38.5% of the respondents stated that the app was no longer needed, while 8 (30.7%) stopped using the app due to data privacy reasons. Out of the 7 people who specified

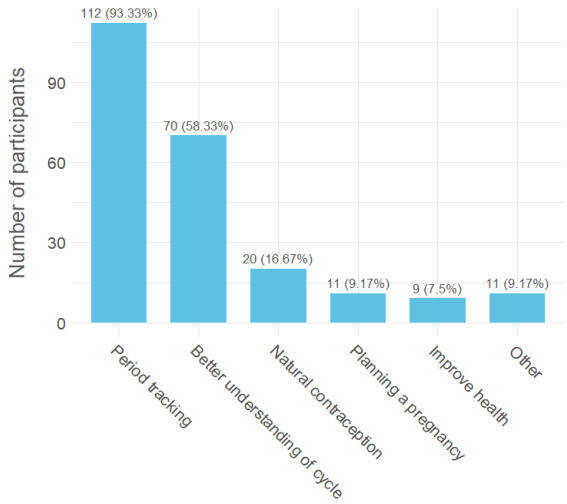

Figure 1 Reasons for using period trackers.

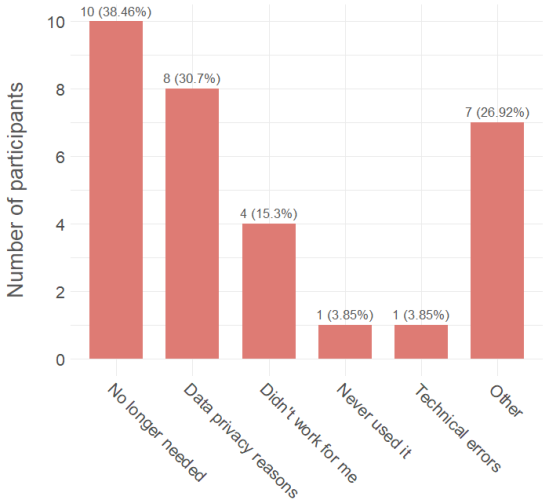

Figure 2 Reasons for discontinuing period trackers.

other reasons, all stated that they currently do not have their period (due to contraception or pregnancy).

Data Privacy Issues and Information Sharing

Despite their potential benefits, the collection, storage, and sharing of personal health data by these digital apps also raise privacy concerns. While the sharing of user data collected through health apps is a common practice, it is currently largely unregulated. For example, in 2022, a study looking at online cancer patient communities found that sensitive health data was funneled through cross-site tracking to Facebook, where it was used for marketing purposes (Downing & Perakslis, 2022). Further, previous research has shown that popular period trackers have significant shortcomings in terms of data privacy, sharing, and security standards. They also fail to comply with regulations of the EU General Data Protection Regulation (GDPR) (Alfawzan et al., 2022). Additionally, a general unease has been expressed about the amount of data and metadata collected and and sold to third parties by most period trackers (Alfawzan et al., 2022). Even before the aforementioned debate surrounding the overturn of Roe v. Wade, data security professionals have warned about the vast amounts of data that these apps collect and sell to third parties, such as Facebook, or even law enforcement agencies, on a large scale (Borges et al., 2018; Mozilla Foundation, n.d.).

» ***Data security professionals have warned about the vast amounts of data that these apps collect and sell to third parties.*** «

Period Trackers and Perceived Privacy Risk

Regardless of these findings, existing research provides an unclear picture of how users *perceive* these issues. On the one hand, some researchers have highlighted a lack of concern among app users when it comes to data privacy and the sharing of personal information. For example, Hohmann-Marriott (2021) found that many users had not given much thought to these issues, deeming them largely unimportant. In a similar vein, a study from the UK showed that particularly among "digital natives", there is a sense of indifference toward data privacy (Broad et al., 2022). Participants saw the sharing of personal data and companies' access to it as standard procedure. On the other hand, research has found that the actual intention to use mHealth applications, such as period trackers, may be heavily influenced by an individual's perceived risks associated with data disclosure, i.e. the belief that the use of mHealth applications may lead to abuse of personal information (Deng et al., 2018).

In that regard, when assessing risk perception in relation to mHealth, *perceived privacy* risk seems especially relevant. Perceived privacy risk refers to the extent to which an individual believes personal information abuse or privacy harm may occur because of mHealth application use (Klaver et al., 2021, p. 2). According to Bhatia & Breaux (2018), there are seven privacy harms leading to perceived privacy risk (see Table 1).

Previous research has found that people are less likely to perceive privacy risks when they are associated with specific benefits, such as lifestyle improvements (Park et al., 2019). This means that individuals who see a great benefit in using mHealth technology are less likely to see privacy risks than those who do not see any benefits.

Table 1 Privacy Harms as in Perceived Privacy Risk.

Appropriation	The feeling of personal information being used unexpectedly
Distortion	The feeling that others are using or sharing inaccurate, misleading, or incomplete information about the user
Induced Disclosure	The feeling of pressure to reveal personal information to others
Insecurity	The feeling that lapses in security aimed at protecting your personal information exist
Surveillance	The feeling of being tracked or monitored
Unanticipated Revelation	The feeling that user information is being revealed or exposed
Unwanted Restriction	The feeling of being unable to access or control personal information

What Did We Find in Our Study?

We measured perceived privacy risk by using the framework of Bhatia and Breaux (2018). Specifically, we asked the participants to what extent they experience the respective privacy harm when using period tracking apps on a scale from 1 to 5.

Overall, our results show a relatively low risk perception in our sample. With 1 being the lowest and 5 the highest value, the participants stated an average perceived privacy risk of *2.3*. Considering the different privacy harms, the feeling of pressure to reveal personal information (*Induced Disclosure*) as well as the feeling of being tracked and monitored (*Surveillance*) were the least prominent. In contrast, users felt more strongly that lapses in security aimed at protecting personal information (*Insecurity*) may exist and that they are unable to access or control their personal information (*Unwanted Restriction*). Although this was not part of our research objectives, we found significant differences between active and past users. Overall, participants who stopped using period trackers reported a 20% higher perceived privacy risk than those who are currently using period trackers.[1] When looking at the reasons why participants had decided to discontinue using the tracking apps, 30.8% stated they stopped due to data privacy reasons. This is in line with previous mHealth research showing that the intention to use depends – among other things – on how individuals perceive privacy risks (Azhar & Dhillon, 2018).

Other studies also demonstrated that when perceived privacy risks are low, they are likely outweighed by the benefits provided by the app (Bhatia & Breaux, 2018; Park et al., 2019). In our case, most active users value being able to track their period as well as better understand their menstrual cycle, especially in relation to co-occurring conditions, such as PMS or endometriosis. This could also be an explanation for higher risk perception in those who do not use the apps anymore since the benefits when using the app could most likely not outweigh the perceived privacy risks anymore.

The Role of Knowledge

Studies on risk perception indicate that having domain-specific knowledge about risks can significantly improve one's ability to evaluate potential hazards. This means that when faced with a potential risk, experts and non-experts tend to approach the situation differently (Siegrist & Árvai, 2020). Experts already possess the required knowledge to make accurate risk assessments, whereas non-experts typically have a more general understanding of the situation, which can lead to an inadequate perception of the risk involved. According to Larsen et al. (2022), more knowledge or

1 We calculated a Wilcoxon rank sum test with $W = 790$, $p < 0.01$, $r = 0.33$.

even awareness of privacy issues can thereby manifest in a lower risk perception regarding data sharing. Others argue that users with the necessary knowledge about data sharing practices may be more likely to tolerate the potential misuse of personal information (Schroeder et al., 2022). In online privacy literacy research, it has also been suggested that users may lack the knowledge to behave in ways that can mitigate the perceived risk (Masur et al., 2017). Overall, there is a scientific argument for knowledge playing a role in shaping our perception of risk. However, there is no consensus on how it specifically influences this perception. In the framework established by Masur et al. (2017), knowledge about online privacy is defined by four pillars, which can be seen in Figure 3.

> ***Individuals with higher perceived knowledge tend to have a lower risk perception.***

For our study, we used the online privacy scale (OPLIS), which is a questionnaire based on the four pillars shown below. This questionnaire captures the knowledge about privacy and data protection regarding online applications. As the questionnaire does not specifically measure knowledge for our domain and no validated scale for knowledge about data privacy and information sharing in mHealth/period tracking apps exists yet, we included five questions for *perceived* knowledge specifically for period trackers.

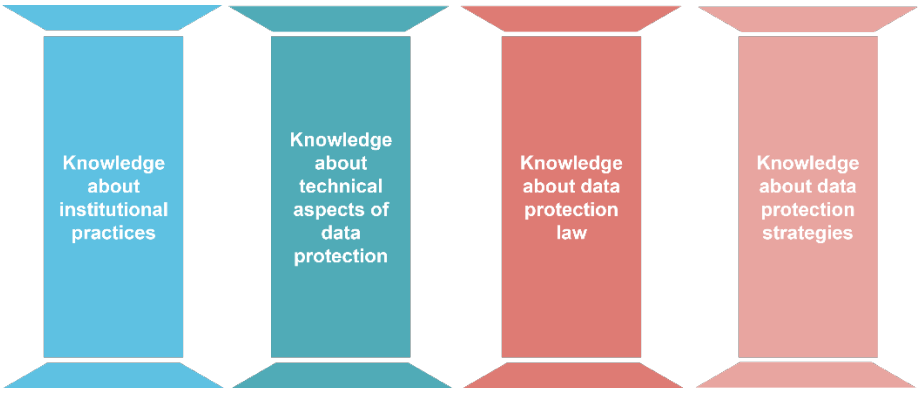

Figure 3 Knowledge of online privacy based on OPLIS (Masur et al., 2017).

What Did We Find?

The knowledge regarding online privacy was surprisingly high among our participants. Interestingly, however, and unlike what previous findings show, our results did not reveal a significant relationship between online privacy literacy and perceived privacy risk. Instead, we found a relationship between perceived domain-specific knowledge and perceived privacy risk, which is visualized in Figure 4. The findings show that individuals with higher perceived knowledge tend to have a lower risk perception. In addition, our results indicate that individuals who discontinued using period trackers have a higher overall risk perception.

Both user groups (active & past) achieved similar results for online data privacy literacy. With an average of 14.54, the respondents overall performed better than 67% of the population according to the findings by Masur et al. (2017). However, while online privacy literacy was not related to risk perception, we found that this was the case for *perceived domain-specific knowledge*. In particular, the more users thought they knew about the data privacy practices of period trackers, the lower their privacy risk perception. Our findings, thus, conform with one of the previous narratives in related research: It can be argued that the majority of regular users are aware of data-sharing practices, but have grown accustomed to those and view them as a normal aspect of using the app (Broad et al., 2022; Hohmann-Marriott, 2021), which may lead to a lower risk perception (Larsen et al., 2022).

This also corresponds with findings on the so-called "privacy paradox": Despite being aware of privacy risks on the internet, many users willingly provide personal information in exchange for goods and personalized services

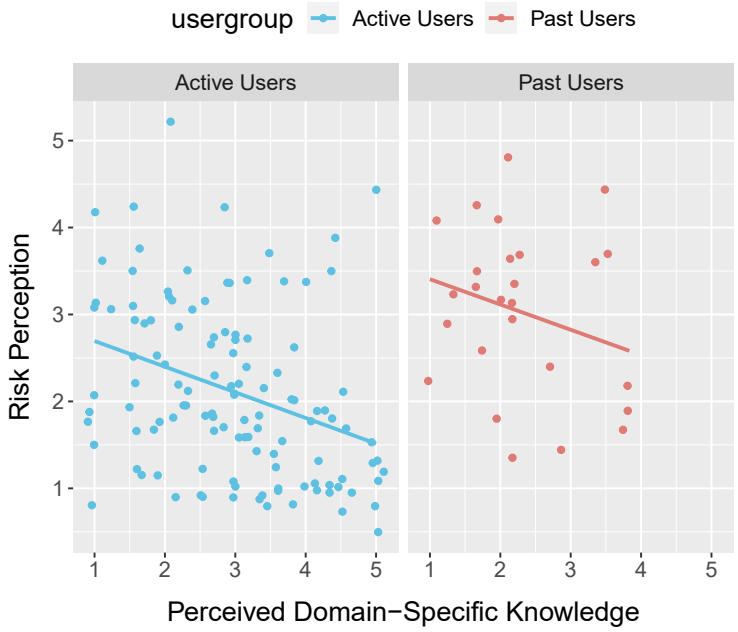

Figure 4 Scatter plot for the relationship between the variables risk perception and perceived domain-specific knowledge. We performed a linear regression analysis and the resulting model explained 15% of the variance in the outcome variable ($R^2 = 0.15$). It should be noted that the sample size for the groups is extremely unbalanced as we did not specifically set out to identify group differences between active and past users.

(Bhatia & Breaux, 2018). We suggest that further research about the privacy paradox regarding period tracking apps is necessary to understand the full picture. In that regard, a comparison between European countries and the US could, for example, reveal differences as to how local laws (e.g., the legal landscape surrounding abortion rights) can affect trade-offs between benefits and risks while using period trackers.

What Could Further Research Look Like?

The limitations of this study are essential to consider when interpreting the findings, as they cannot be generalized. First and foremost, our survey was conducted in German. The personal data of German citizens is protected by the GDPR, so users may have a lower perception of data sharing risks since they know that their data is protected – at least to some degree. In the future, comparative studies with, e.g., the US may, hence, be informative. Further, it should be noted that with measuring *perceived* domain-specific knowledge, our results cannot provide information about whether the perception of knowledge or the actual knowledge of data sharing in period trackers was responsible for the correlation with risk perception. This would be interesting to further disentangle in future research. The type of apps that respondents were using may also play an essential role. In our study, the most commonly used period tracker was *Clue* with 27.4%. According to the Mozilla Foundation (n.d.), *Clue* is based in Germany, and its data use is governed by the European GDPR. However, nearly 20% used *Flo*, which attracted negative attention by sharing sensitive data with Facebook without prior disclosure (Gupta & Singer, 2021). Flo Health Inc., the company behind Flo App was founded in Belarus with current headquarters in England and USA (*Flo App, Inc.*, n.d.; Khidekel, 2018). The relationship between different data privacy regulations of individual apps and perceived risk could be explored in further research.

Key Messages

Our study found that active users of period trackers have a relatively low perception of risks concerning data privacy and information sharing, while those who have stopped using such apps perceive the risks to be significantly higher. Our findings, thus, align with previous studies in mHealth research which have shown that the actual intention to use an app can be related to how individuals perceive privacy risks. Additionally, perceived domain-specific knowledge was associated with lower risk perception in our study.

In terms of practical implications for users, our results suggest that it is important for individuals to consider the data privacy and sharing practices of different companies when choosing a period tracker. This is particularly crucial in light of recent changes to laws surrounding reproductive rights in several countries, including the US, and to ensure the protection of personal privacy. The study by the Mozilla Foundation (n.d.) highlights clear distinctions between different apps in terms of their data sharing practices and privacy regulations, and this is something that users should consider when deciding on an app.

References

Alfawzan, N., Christen, M., Spitale, G., & Biller-Andorno, N. (2022). Privacy, data sharing, and data security policies of women's mHealth apps: Scoping review and content analysis. *JMIR MHealth and UHealth, 10*(5), e33735. https://doi.org/10.2196/33735

Azhar, F., & Dhillon, J. S. (2018). An investigation of factors influencing the intention to use mHealth apps for self-care. *International Journal of Business Information Systems, 29*, 59. https://doi.org/10.1504/IJBIS.2018.094005

Bhatia, J., & Breaux, T. D. (2018). Empirical measurement of perceived privacy risk. *ACM Transactions on Computer-Human Interaction, 25*(6), 34:1-34:47. https://doi.org/10.1145/3267808

Borges, A. L. V., Moreau, C., Burke, A., Santos, O. A. dos, & Chofakian, C. B. (2018). Women's reproductive health knowledge, attitudes and practices in relation to the Zika virus outbreak in northeast Brazil. *PLOS ONE, 13*(1), e0190024. https://doi.org/10.1371/journal.pone.0190024

Broad, A., Biswakarma, R., & Harper, J. C. (2022). A survey of women's experiences of using period tracker applications: Attitudes, ovulation prediction and how the accuracy of the app in predicting period start dates affects their feelings and behaviours. *Women's Health, 18*. https://doi.org/10.1177/17455057221095246

Deng, Z., Hong, Z., Ren, C., Zhang, W., & Xiang, F. (2018). What predicts patients' adoption intention toward mHealth services in China: Empirical study. *JMIR MHealth and UHealth, 6*(8), e9316. https://doi.org/10.2196/mhealth.9316

Downing, A., & Perakslis, E. (2022). Health advertising on Facebook: Privacy and policy considerations. *Patterns, 3*(9), 100561. https://doi.org/10.1016/j.patter.2022.100561

Flo App, Inc. (n.d.). Flo.health - #1 mobiles Produkt für die weibliche Gesundheit. Retrieved June 12, 2023, from https://flo.health/de/kontakt

Gupta, A. H., & Singer, N. (2021, January 28). Your app knows you got your period. Guess who it told? *The New York Times.* https://www.nytimes.com/2021/01/28/us/period-apps-health-technology-women-privacy.html

Healy, R. L. (2021). Zuckerberg, get out of my uterus! An examination of fertility apps, data-sharing and remaking the female body as a digitalized reproductive subject. *Journal of Gender Studies, 30*(4), 406–416. https://doi.org/10.1080/09589236.2020.1845628

Hohmann-Marriott, B. (2021). Periods as powerful data: User understandings of menstrual app data and information. *New Media & Society.* https://doi.org/10.1177/14614448211040245

Khidekel, Marina. (2018, June 25). *The race to hack your period is on*. ELLE. https://www.elle.com/beauty/health-fitness/a21272099/clue-period-app/

Klaver, N. S., van de Klundert, J., van den Broek, R. J. G. M., & Askari, M. (2021). Relationship between perceived risks of using mHealth applications and the intention to use them among older adults in the Netherlands: Cross-sectional study. *JMIR MHealth and UHealth, 9*(8), e26845. https://doi.org/10.2196/26845

Larsen, M. H., Lund, M. S., & Bjørneseth, F. B. (2022). A model of factors influencing deck officers' cyber risk perception in offshore operations. *Maritime Transport Research, 3*, 100065. https://doi.org/10.1016/j.martra.2022.100065

Levy, J., & Romo-Avilés, N. (2019). "A good little tool to get to know yourself a bit better": A qualitative study on users' experiences of app-supported menstrual tracking in Europe. *BMC Public Health, 19*(1), 1213. https://doi.org/10.1186/s12889-019-7549-8

Masur, P. K., Teutsch, D., & Trepte, S. (2017). Entwicklung und Validierung der Online-Privatheitskom-

petenzskala (OPLIS). *Diagnostica, 63*(4), 256–268. https://doi.org/10.1026/0012-1924/a000179

Mozilla Foundation. (n.d.). **Privacy not included: A buyer's guide for connected products*. https://foundation.mozilla.org/en/privacynotincluded/

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., & Patsakis, C. (2018). Security and privacy analysis of mobile health applications: The alarming state of practice. *IEEE Access, 6*, 9390–9403. https://doi.org/10.1109/ACCESS.2018.2799522

Park, J., Amendah, E., Lee, Y., & Hyun, H. (2019). M-payment service: Interplay of perceived risk, benefit, and trust in service adoption. *Human Factors and Ergonomics in Manufacturing & Service Industries, 29*(1), 31–43. https://doi.org/10.1002/hfm.20750

Schnall, R., Higgins, T., Brown, W., Carballo-Dieguez, A., & Bakken, S. (2015). Trust, perceived risk, perceived ease of use and perceived usefulness as factors related to mHealth technology use. *Studies in Health Technology and Informatics, 216*, 467–471.

Schroeder, T., Haug, M., & Gewald, H. (2022). Data privacy concerns using mHealth apps and smart speakers: Comparative interview study among mature adults. *JMIR Formative Research, 6*(6), e28025. https://doi.org/10.2196/28025

Siegrist, M., & Árvai, J. (2020). Risk perception: Reflections on 40 years of research. *Risk Analysis, 40*(S1), 2191–2206. https://doi.org/10.1111/risa.13599

Somberg, T. (2022). *Living in a Post-Roe V. Wade world: Can your period tracker app data be used against you? - Exclusive*. Women. https://www.women.com/1242703/can-your-period-tracker-app-data-be-used-against-you/

Annika Deubel

Center for Advanced Internet Studies (CAIS)

E-Mail: annika.deubel@cais-research.de

Annika Deubel is a doctoral researcher at the Center for Advanced Internet Studies (CAIS) in Bochum, Germany. In her research, she focuses on health information on social media. She is generally interested in computational methods and digital behavioural data.

Pauline Heger

Center for Advanced Internet Studies (CAIS)

E-Mail: pauline.heger@cais-research.de

Pauline Heger is a doctoral researcher at the Center for Advanced Internet Studies (CAIS) in Bochum, Germany, with a background in communication science. Her research focuses on social diffusion of innovation, sustainable technologies, and HCI.