"It doesn't just feel like something a lawyer slapped together."- Mental-Model-Based Privacy Policy for Third-Party Applications on Facebook

Rizu Paudel
rizu.paudel@usu.edu
Utah State University
Logan, Utah, USA

Ankit Shrestha
ankit.shrestha@usu.edu
Utah State University
Logan, Utah, USA

Prakriti Dumaru
prakriti.dumaru@usu.edu
Utah State University
Logan, Utah, USA

Mahdi Nasrullah Al-Ameen
mahdi.al-ameen@usu.edu
Utah State University
Logan, Utah, USA

ABSTRACT

Users are often unaware of the information that applications collect and are surprised by unexpected data collection and sharing practices. With numerous third-party applications on Facebook potentially accessing the personal information of billions of users, it is essential to understand users' mental models of data sharing to help them make informed decisions. To achieve this, we conducted semi-structured interviews using drawings and think-aloud protocol with 32 participants. Our participants had misconceptions regarding third-party applications' data sharing practices with varied mental models. Based on these findings, we created mental model-based privacy policy design that prompts users to consider a specific scenario and provides information to help them understand their misconceptions. To evaluate our designs, we then conducted an online study with 26 participants over Amazon Mechanical Turk (MTurk). Our results showed that using mental models helped users comprehend the message in the privacy policy, connect them to the design, and grabbed their attention. Finally, we offer recommendations for future research regarding the usage of mental models in designs to combat users' misconceptions with an effortless depiction of privacy policy.

CCS CONCEPTS

• **Human-centered computing** → **Human computer interaction (HCI)**; • **Security and privacy** → **Usability in security and privacy**.

KEYWORDS

Mental models; Third-party applications; Privacy Policy Design; User Studies

CSCW '23 Companion, October 14–18, 2023, Minneapolis, MN, USA

ACM ISBN 979-8-4007-0129-0/23/10.
https://doi.org/10.1145/3584931.3606962

ACM Reference Format:
Rizu Paudel, Ankit Shrestha, Prakriti Dumaru, and Mahdi Nasrullah Al-Ameen. 2023. "It doesn't just feel like something a lawyer slapped together."- Mental-Model-Based Privacy Policy for Third-Party Applications on Facebook. In *Computer Supported Cooperative Work and Social Computing (CSCW '23 Companion), October 14–18, 2023, Minneapolis, MN, USA.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3584931.3606962

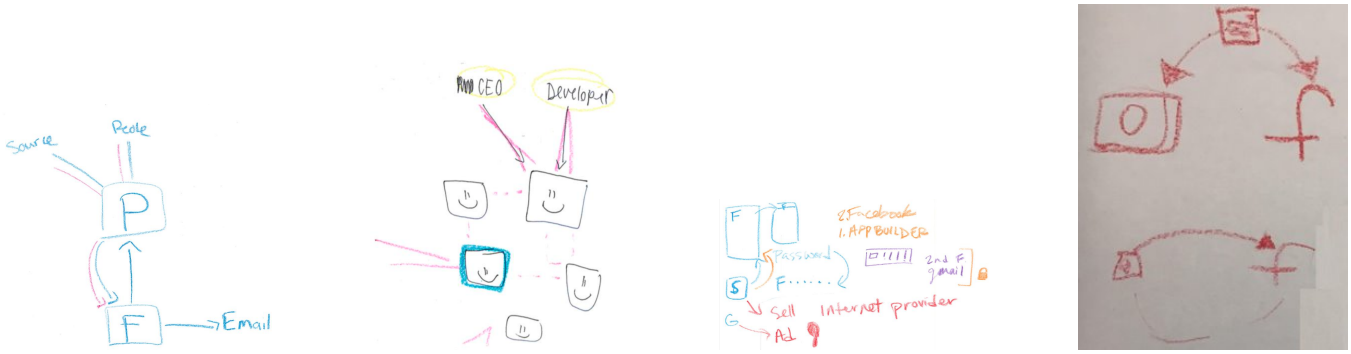
1 INTRODUCTION

Online social networks such as Facebook have millions of third-party applications on their platforms [10, 13]. These third-party applications can get access to billions of accounts including the personal information of users who install these apps [12]. The lack of proper conceptual models leads to the misconceptions of users about the intended use and working mechanism of computing technologies [23, 24]. In the case of third-party applications on Facebook, such misconceptions may not only pose usability constraints, but also raise concerns about the protection of user information and credentials. According to the research conducted by Forget et al. [15], the inappropriate use of technology can be attributed to the fact that there is a gap in users' understanding of the tools designed for them [15]. This highlights the importance of understanding users' mental model by examining users' comprehension and identifying their misconceptions concerning these applications. In another study [21], participants perceived that the government and giant tech-based companies could access their personal data anytime they want; such belief is fueled by the personalized ads and product recommendations shown to users while browsing the Internet. To this end, we aim to categorize users based on their mental models, and leverage that understanding to design the privacy policy to clear their misconceptions about these applications. In particular, we address the following research questions in our study.

RQ1: How can we categorize users' mental model based on their perceptions of third-party applications on Facebook?

RQ2: How can we use the mental models of users to design a privacy policy for third-party applications on Facebook?

RQ3: How effective is a mental model-based privacy policy design in engaging and connecting with users?



(a) Single Sign-On (b) Person in the Back (c) Information Sharing (d) Shared Ownership

Figure 1: Participants' Mental Model Drawing Categorization

We conducted semi-structured interviews and a drawing task-based lab study with 32 participants to investigate their understanding and misconceptions about third-party applications on Facebook, and their mental models related to data sharing practices (**RQ1**; see §2.2). Based on our results, we categorized users' mental model and then created designs for privacy policy (**RQ2**; see §2.2), which were evaluated in an online study with 26 participants over MTurk. The findings from our study show promise in leveraging users' mental models to design privacy policy, where we found significant differences with the control condition in almost all parameters, including users' attention, participant's sense of connection with the privacy policy interface, novelty, and aesthetics (**RQ3**; see §3.2). Our designs received positive feedback from participants, who reported a willingness to adopt them in real life. We also offer recommendations for future research on using mental models in designs to help users understand their misconceptions about privacy policies.

2 LAB STUDY

2.1 Methodology: Users' Mental Model

We conducted semi-structured interviews with 32 adult participants in the USA, where anyone above 18 years (self-reported) could participate (see Table 2 for details). Participants were recruited using the online platform created by our university for human-subject studies and through email listservs of the local community. The Institutional Review Board (IRB) at our university approved our study. The study was conducted in person at our university lab. Participants were first presented with an Informed Consent Document (ICD) following a short survey on their usage of the Internet and third-party applications on Facebook. They were asked to draw a diagram of third-party applications on Facebook and verbalize their thought process using traditional think-aloud protocols [11]. Participants were then interviewed about their perceptions of data access by different entities and asked follow-up questions. A video camera captured participants' drawings and voices. The session took 30-60 minutes, and participants were compensated with a $15 Amazon.com Gift Card. We did not collect any personally identifiable information.

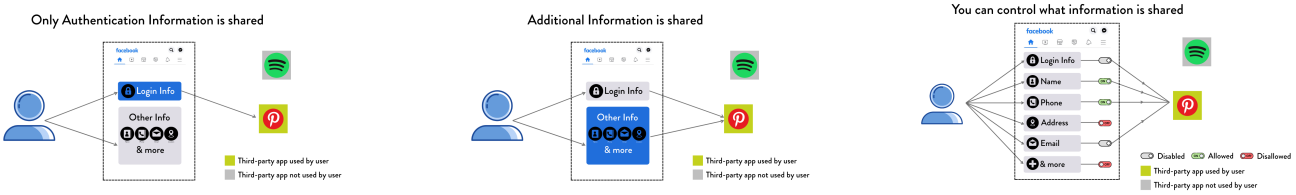
We analyzed the interviews of our participants by transcribing and qualitatively analyzing their drawings and audio recordings using thematic analysis [6–8]. We took an inductive approach, developing codes from the data of the first few participants, iteratively comparing and finalizing a codebook, and then independently coding all participants' data. Two researchers spot-checked each other's coded data and found no inconsistencies. We then organized and categorized our codes into higher-level categories.

2.2 Results: Mental Model Categorization

In this section, we present the findings from our lab study where we categorized participants' mental model based on their drawings and interviews. We also highlight participants' misconceptions and how they informed our mental model based privacy policy design for data sharing practices of third-party applications on Facebook.

Sign-On Information Sharing. Some participants held misconceptions about the information shared with third-party applications when using Facebook to sign up, including the belief that only authentication information was shared. We used their mental model to create designs that prompted them to indicate their understanding of information sharing and provided correct information (Figure 4), demonstrating that not only authentication information but also additional information is shared as shown in Figure 5b. They also thought that their credentials were stored on Facebook's server and shared with third-party apps. P29 in the context of signing up for Spotify using Facebook said, *"...it's kind of saying, "Hey Facebook...do you know this person?" and be like, "Oh yeah totally we have their password and everything," and they'll be like, "Ok sweet get that to us," and then you can sign in with your Facebook..."* To address this misconception, we created a design that provided information on how the login process works through authentication tokens and that passwords are not shared during authentication (see Figure 5h).

Data is Shared with Entities in Power. Participants believed that the information they share with third-party applications on Facebook can be accessed by various entities, including developers, large tech companies, and government agencies and that they have no control over their data-sharing practices (see Figure 1c). P29 said, *"It definitely goes to Facebook...because you're signing in with Facebook, they can see it...the app builder [developer]...definitely...probably would go to the app builder first just because like that's where it's coming in...maybe the NSA...and then maybe your internet provider..."* To address this misconception, we created a design that showed



(a) Single Sign-On **(b) Additional Sharing** **(c) Data Control**

Figure 2: Treatment Conditions: Mental Model based Designs [Note: The figure only contains three out of ten scenarios, where all ten scenarios is included in Appendix of the paper]

the characters participants mentioned and provided information on how they can control their data-sharing practices (see Figure 5f).

Profit based Sharing. Some participants believed that Facebook was sharing their information with third-party apps for profit, which created a misconception about their data control. Our design aimed to clarify that by providing information on how Facebook does not sell personal information to third-party apps, but may share anonymized reports with advertisers (see Figure 5d). For instance, P8 said, *"...Facebook can approach third party...then sell the rights to advertise...so that they can make money...and...[they want me to]...buy whatever it is they are selling that makes them money...so that's how that works...they can also sell information regarding their customers to other corporations and stuff..."*

Shared Ownership. Participants in our study believed that Facebook, Instagram, and WhatsApp, all owned by same company, shares a common server where information is shared between companies (see Figure 1d). P10 said, *"...there's Facebook and then whoever...owns Facebook also has Instagram...they work together to share data between the two to figure out...followers and stuff..."* Some participants also thought there might be a key token or certificate connecting Instagram to Facebook. To address this misconception, our design showed how information is shared between companies with the same ownership and clarified that they do not have the same storage but share infrastructure, systems, and technology within Meta companies (see Figure 5g).

Person in the Back. Participants misunderstood how background data management and sharing occurs between Facebook and third-party applications, believing that manual intervention was necessary. For instance, P32 stated, *"...Facebook...has...their own software development team...third party applications through Facebook...will have to get permission from Facebook to transfer their data to the server, then a team of software developers will...upload that to their Facebook..."* To address this misconception, we included an icon of developer in our design and provided information that data sharing with third-party applications is automated without manual intervention (see Figure 5e).

Bidirectional Flow of Data. Participants had a misconception that data flows bidirectionally between third-party applications and Facebook. For instance, P25 commented, *"...it's kind of...like...connected circuit...connects everything about Facebook with that system, and everything about that system [third-party apps] with Facebook."* To address this misconception, we provided information on the partial sharing of data, clarifying that third-party applications only have access to the data they request and not all data provided to Facebook is shared (see Figure 5i).

3 ONLINE STUDY

3.1 Methodology: Survey

We conducted an online study via MTurk to evaluate our designs and compare them with a control condition. Our study was approved by the IRB at our university. For participant recruitment, we considered a large effect size in our power analysis, where a sample size of 26 is adequate per study condition (Cohen's d=0.8, alpha=0.05, and Power=80%) [9]. We continued recruiting participants until we got at least 26 participants who did not fail any attention checks (see Table 3). For our study, we designed a survey system in Qualtrics where the participants were first asked to read an ICD.

In our study, we employed a within-subject approach where the participants interacted and evaluated both control and treatment conditions. Firstly, participants interacted with a control condition that presented Facebook's existing privacy policy in a textual format. They were then asked to evaluate it using a 7-point Likert scale (1: strongly disagree, 7: strongly agree). Following this evaluation, participants interacted with the treatment condition as shown in Figure 4 in Appendix. The treatment condition comprised a total of ten illustrations, derived from participants' mental models in the lab study. A selection of three out of the ten illustrations is shown in Figure 5. Upon completing the interaction of each illustration in the treatment condition, participants provided an evaluation of the treatment condition, following a similar approach. Participants were specifically asked to evaluate the design based on its *Novelty*, *Perspicuity*, and *Aesthetics* [29] using a validated scale (e.g., UEQ+ [30]). We also asked them about how effective the design was in grabbing their attention (*User Attention*) and making them feel connected with the design (*Personal Connection*) by adding custom questions similar to prior studies [14, 34, 35]. Participants were also asked about their inclination to adopt the design in real life and responded to open-ended questions to provide feedback on the presented designs. They then answered a set of demographic questions and were compensated with $2.00 for completing the study, which took an average of 12 minutes.

Measures	Test Statistic
Perspicuity	Z=-1.24, p=0.21
Novelty	**Z=-3.86, p<0.05**
Aesthetics	**Z=-2.83, p<0.05**
User Attention	**Z=-3.23, p<0.05**
Personal Connection	**Z=-2.30, p<0.05**

Table 1: Significance Test Results

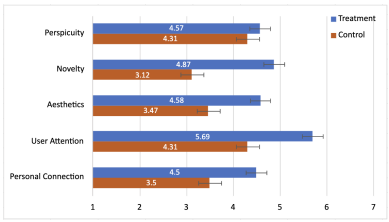


Figure 3: Mean of Participants' Ratings for Control and Treatment Conditions

3.2 Results: Design Evaluation

We used non-parametric Wilcoxon Signed-Rank tests for matched pairs since our data was not normally distributed. We also performed thematic analysis [7, 8] on open-ended responses from participants. Our designs are rated positively (on average) by participants on all the measures (Figure 3); we compared our designs with a control condition and found significant differences on all measures except for Perspicuity (Table 1). Participants also expressed positive likelihood towards adopting our design in real-life scenarios (M=4.88, SD=1.53).

Design helped me feel connected. Participants felt a stronger connection to the treatment condition compared to the control condition, with a significant difference between the two (see Table 1). They appreciated the design that suited their learning preferences, with one participant expressing that visual aids helped them understand better. Participants also felt a personal connection to the design, with some saying that scenarios made them feel like a user in the design, and they could imagine their information being shared as shown in the design. We also found that participants felt a stronger connection to the design due to its use of familiar visual cues: *"...[it's] easy to understand and things I see in my everyday life, it makes the connection between the info and me a bit stronger because I can relate to the icons."*. Participants also expressed that our design gave them a sense of control over protecting their online privacy.

Design grabbed my attention. We found significantly higher rating for treatment than control condition in terms of capturing attention of participants towards the privacy policies of third party applications on Facebook (see Table 1). Participants found the visual representation of the privacy policy more engaging and easier to understand. They mentioned that the visuals were better and easier to digest than large blocks of text, which can be intimidating. Participants also felt that the design was tailored to their audience, making it more user-friendly and inviting them to engage with the information provided. Overall, the privacy policy design was found to be more user-friendly, encouraging individuals to take responsibility for their privacy.

Design helped in better comprehension. Participants rated treatment condition higher than the control condition for *Perspicuity* (see Figure 3). They appreciated the simplicity of our design where one of them commented, *"I like how the designs try to make things simple and understandable, so you can know in a simple way, how your data is used and what you can and can't do, and what others can and can't do...It makes me feel like I have a little more control over my information..."* Participants also mentioned on the ease of understanding and following the information, stating that our design is better than the existing policy, which they found monotonous and time-consuming.

Design is novel and appealing. Our design was rated significantly higher than the control condition in terms of its *Novelty* and *Aesthetics* (Table 1). Participants found it appealing, creative, and trustworthy, with characters such as icons making it easier to understand. They appreciated how our design taught them about third-party applications in a more accessible way, compared to plain text. Participants also appreciated the novelty of our design, where they mentioned how our design felt intuitive compared to a legal document, making it easier to remember and trust: *"It feels much more modern and intuitive. It doesn't just feel like something a lawyer slapped together. It seems easier to remember and more trustworthy."*. Another participant echoed these sentiments, stating that our design was visually appealing and engaging compared to the control condition.

4 DISCUSSION

4.1 Mental Model Based Design

Our study revealed that users have misconceptions about third-party applications data sharing practices on Facebook. We suggest highlighting the importance of mental model-based designs to address these misconceptions in this section. We also recommend further research in this area to explore additional ways of addressing the users' misconceptions.

Mental Model Cognizance. We found that incorporating mental models into system design is an effective approach to address users' misconceptions that can help users make informed security decisions. Prior studies have shown that users have diverse mental models of privacy and security [21, 22, 25, 33], and designing systems with these models in mind is crucial to assist users in aligning their mental models with the system's design [4, 31]. However, mental model integration into system design is often lacking. In our study, we categorized users' mental models based on common misconceptions and built our design around them. Our results indicate that mental model-based designs can help users make better online security decisions. Our participants' willingness to adopt mental model-based privacy policies in real-life suggests that these designs should be explored and evaluated for a broader range of security and privacy decision-making contexts, including security warnings, password creation, and software updates.

Effortless Depiction. In our privacy policy design, we used icons to represent different entities involved in sharing and accessing users' information, such as users themselves, developers, government, Facebook, and third-party applications. The characters in our designs are influenced by users' mental models and drawings (see 2.2). Prior research has suggested that privacy icons can improve users' comprehension of privacy-related information [16, 19, 20]. We found that participants responded positively to the icons we used, and also found them relatable and attention-grabbing. They also felt more connected to the information presented, as they could imagine themselves in the depicted situations. The use of relatable characters and icons helped emphasize the importance of privacy and security; thus, we believe, depiction of characters, icons relating to users was a key component contributing to user attachment and engagement with our design.

Combating Misconceptions. We found that participants held a variety of misconceptions regarding the data-sharing practices of third-party applications on Facebook, which is consistent with a previous study conducted by Kang et al. [21], where participants believed that their personal data could be accessed at any time by government agencies and large tech companies. Prior studies have shown that users place high importance on how their data is collected, used, and disclosed by online platforms [5, 17, 27, 28]. Our research specifically focused on the data sharing practices of third-party applications on Facebook. While some of our findings are consistent with prior research [21] indicating that users often have misconceptions about data privacy and security, further research is necessary to uncover the various mental models that users hold and how they impact users' understanding and decision-making. Conducting a field study using a diary-based approach could help to identify the root causes of these misconceptions and contribute to the HCI community's efforts to help users understand and eliminate incorrect mental models.

4.2 Limitations and Future Work

In our lab study, we used established qualitative research methods [6–8], however, to obtain measurable outcomes, we conducted an online study to evaluate our mental model-based designs in a controlled environment. Although a controlled environment may not reflect real-world behavior, it can establish performance boundaries. Given the promising results, future research should test users' navigation of mental-model-based privacy policies in real-world settings. Additionally, our study was limited to U.S. participants, so future studies should look beyond Western contexts to understand users' mental models, which can vary significantly across different geographic locations [1–3, 18, 26, 32].

ACKNOWLEDGMENTS

We would like to thank the reviewers for their valuable feedback. This material is based upon work supported by the National Science Foundation under Award No. CNS-1949699.

REFERENCES

[1] Mahdi Nasrullah Al-Ameen and Huzeyfe Kocabas. 2020. "I cannot do anything": User's Behavior and Protection Strategy upon Losing, or Identifying Unauthorized Access to Online Account. In *Symposium on Usable Privacy and Security (Poster Session).*

[2] Mahdi Nasrullah Al-Ameen, Huzeyfe Kocabas, Swapnil Nandy, and Tanjina Tamanna. 2021. "We, three brothers have always known everything of each other": A Cross-cultural Study of Sharing Digital Devices and Online Accounts. *Proceedings on Privacy Enhancing Technologies* 2021, 4 (2021), 203–224.

[3] Mahdi Nasrullah Al-Ameen, Tanjina Tamanna, Swapnil Nandy, M. A. Manazir Ahsan, Priyank Chandra, and Syed Ishtiaque Ahmed. 2020. We Don't Give a Second Thought Before Providing Our Information: Understanding Users' Perceptions of Information Collection by Apps in Urban Bangladesh. In *Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies* (Ecuador) *(COMPASS '20).* Association for Computing Machinery, New York, NY, USA, 32–43. https://doi.org/10.1145/3378393.3402244

[4] Hanieh Atashpanjeh, Arezou Behfar, Cassity Haverkamp, Maryellen McClain Verdoes, and Mahdi Nasrullah Al-Ameen. 2022. Intermediate Help with Using Digital Devices and Online Accounts: Understanding the Needs, Expectations, and Vulnerabilities of Young Adults. In *HCI for Cybersecurity, Privacy and Trust: 4th International Conference, HCI-CPT 2022, Held as Part of the 24th HCI International Conference, HCII 2022, Virtual Event, June 26–July 1, 2022, Proceedings.* Springer, 3–15.

[5] Rebecca Balebako, Richard Shay, and Lorrie Faith Cranor. 2014. Is your inseam a biometric? a case study on the role of usability studies in developing public policy. *Proc. USEC* 14 (2014).

[6] Kathy Baxter, Catherine Courage, and Kelly Caine. 2015. *Understanding your users: a practical guide to user research methods.* Morgan Kaufmann.

[7] Richard E Boyatzis. 1998. *Transforming qualitative information: Thematic analysis and code development.* sage.

[8] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[9] Jacob Cohen. 2013. *Statistical power analysis for the behavioral sciences.* Academic press.

[10] Brittany Darwell. 2012. Facebook platform supports more than 42 million pages and 9 million apps. *Inside Facebook, April* (2012).

[11] K Anders Ericsson and Herbert A Simon. 1980. Verbal reports as data. *Psychological review* 87, 3 (1980), 215.

[12] Facebook. Year Published. *Permissions with Facebook Login.* https://developers.facebook.com/docs/facebook-login/guides/permissions

[13] Shehroze Farooqi, Maaz Musa, Zubair Shafiq, and Fareed Zaffar. 2020. Canarytrap: Detecting data misuse by third-party apps on online social networks. *arXiv preprint arXiv:2006.15794* (2020).

[14] Matthias Fassl, Lea Theresa Gröber, and Katharina Krombholz. 2021. Exploring user-centered security design for usable authentication ceremonies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems.* 1–15.

[15] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. 2016. Do or do not, there is no try: user engagement may not improve security outcomes. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016).* 97–111.

[16] Armin Gerl. 2018. Extending layered privacy language to support privacy icons for a personal privacy policy user interface. In *Proceedings of the 32nd International BCS Human Computer Interaction Conference 32.* 1–5.

[17] Hana Habib, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Joel Reidenberg, Norman Sadeh, and Florian Schaub. 2021. Toggles, dollar signs, and triangles: How to (in) effectively convey privacy choices with icons and link texts. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems.* 1–25.

[18] S. M. Taiabul Haque, Md Romael Haque, Swapnil Nandy, Priyank Chandra, Mahdi Nasrullah Al-Ameen, Shion Guha, and Syed Ishtiaque Ahmed. 2020. Privacy Vulnerabilities in Public Digital Service Centers in Dhaka, Bangladesh. In *Proceedings of the 2020 International Conference on Information and Communication Technologies and Development* (Guayaquil, Ecuador) *(ICTD2020).* Association for Computing Machinery, New York, NY, USA, Article 14, 12 pages. https://doi.org/10.1145/3392561.3394642

[19] Leif-Erik Holtz, Katharina Nocun, and Marit Hansen. 2011. Towards displaying privacy information with icons. In *Privacy and Identity Management for Life: 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010, Revised Selected Papers 6.* Springer, 338–348.

[20] Leif-Erik Holtz, Harald Zwingelberg, and Marit Hansen. 2011. Privacy policy icons. In *Privacy and Identity Management for Life.* Springer, 279–285.

[21] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015).* 39–52.

[22] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. 2020. User Mental Models of Cryptocurrency Systems — A Grounded Theory Approach. In *USENIX Symposium on Usable Privacy and Security (SOUPS).* 341–358.

[23] Donald A Norman. 1991. Cognitive artifacts. *Designing interaction: Psychology at the human-computer interface* 1, 1 (1991), 17–38.

[24] Donald A Norman. 1999. Affordance, conventions, and design. *interactions* 6, 3 (1999), 38–43.
[25] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. 2018. Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration. *Proceedings on Privacy Enhancing Technologies* 2018, 4 (2018), 5–32.
[26] Rizu Paudel, Prakriti Dumaru, Ankit Shrestha, Huzeyfe Kocabas, and Mahdi Nasrullah Al-Ameen. 2023. A Deep Dive into User's Preferences and Behavior around Mobile Phone Sharing. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW1 (2023), 1–22.
[27] Daniel Reinhardt, Johannes Borchard, and Jörn Hurtienne. 2021. Visual Interactive Privacy Policy: The Better Choice?. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–12.
[28] Arianna Rossi and Monica Palmirani. 2019. DaPIS: A data protection icon set to improve information transparency under the GDPR. *Knowledge of the Law in the Big Data Age* 252, 181-195 (2019), 5–5.
[29] Martin Schrepp, Andreas Hinderks, and Jörg Thomaschewski. 2014. Applying the user experience questionnaire (UEQ) in different evaluation scenarios. In *International Conference of Design, User Experience, and Usability*. Springer, 383–392.
[30] Martin Schrepp and Jörg Thomaschewski. 2019. Handbook for the modular extension of the User Experience Questionnaire. *Retrieved from www. ueq-online. org* (2019).
[31] Ankit Shrestha, Danielle M Graham, Prakriti Dumaru, Rizu Paudel, Kristin A Searle, and Mahdi Nasrullah Al-Ameen. 2022. Understanding the Behavior, Challenges, and Privacy Risks in Digital Technology Use by Nursing Professionals. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–22.
[32] Sharifa Sultana, Pratyasha Saha, Shaid Hasan, S. M. Raihanul Alam, Rokeya Akter, Md. Mirajul Islam, Raihan Islam Arnob, Mahdi Nasrullah Al-Ameen, and Syed Ishtiaque Ahmed. 2020. Understanding the Sensibility of Social Media Use and Privacy with Bangladeshi Facebook Group Users. In *Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies* (Ecuador) *(COMPASS '20)*. Association for Computing Machinery, New York, NY, USA, 317–318. https://doi.org/10.1145/3378393.3402235
[33] Justin Wu and Daniel Zappala. 2018. When is a tree really a truck? exploring mental models of encryption. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS)*. 395–409.
[34] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. 2013. Password advice shouldn't be boring: Visualizing password guessing attacks. In *2013 APWG eCrime Researchers Summit*. 1–11. https://doi.org/10.1109/eCRS.2013.6805770
[35] Verena Zimmermann, Karola Marky, and Karen Renaud. 2022. Hybrid password meters for more secure passwords–a comprehensive study of password meters including nudges and password information. *Behaviour & Information Technology* (2022), 1–44.

5 APPENDIX

PID	Gender	Age Range	Academic Background
P01	F	30-34	School Counseling Med
P02	F	18-24	Human Biology
P03	M	25-29	N/A
P04	F	18-24	Parks and Rec
P05	F	18-24	N/A
P06	M	18-24	History
P07	M	18-24	Psychology
P08	F	18-24	Communicative Disorders
P09	M	25-29	Technology Systems
P10	M	18-24	Business Management
P11	F	18-24	ELED
P12	M	18-24	Pre-Business
P13	F	18-24	Psychology
P14	M	25-29	Nursing
P15	M	18-24	Biology
P16	M	18-24	Psychology
P17	F	18-24	Human Dev. Studies
P18	F	18-24	Psychology
P19	F	18-24	Health Science
P20	F	18-24	Prephysical Therapy
P21	F	18-24	Psychology
P22	F	18-24	Undecided (Exploratory)
P23	F	18-24	Finance
P24	F	18-24	N/A
P25	F	18-24	Art
P26	M	18-24	Business
P27	M	18-24	Landscape Architecture
P28	M	18-24	N/A
P29	F	18-24	Accounting & Math
P30	M	18-24	Bio Engineering
P31	M	35-39	Civil Engineering
P32	M	25-29	Computer Science

Table 2: Lab Study: Demographic Information of Participants (N = 32)

Demographics		Number of Participants
Gender	Male	18
	Female	8
Age range	30-34 years old	4
	35-39 years old	9
	40-44 years old	5
	45-49 years old	2
	50-54 years old	2
	55-59 years old	1
	60-64 years old	1
	Above 65 years old	2
Race	White	23
	Asian	1
	Black/African American	1
	Mixed Race	1
Education Level	High school graduate	5
	Two-year college degree	7
	Four-year college degree	14

Table 3: Online Study: Demographic Information of Participants (N = 26)

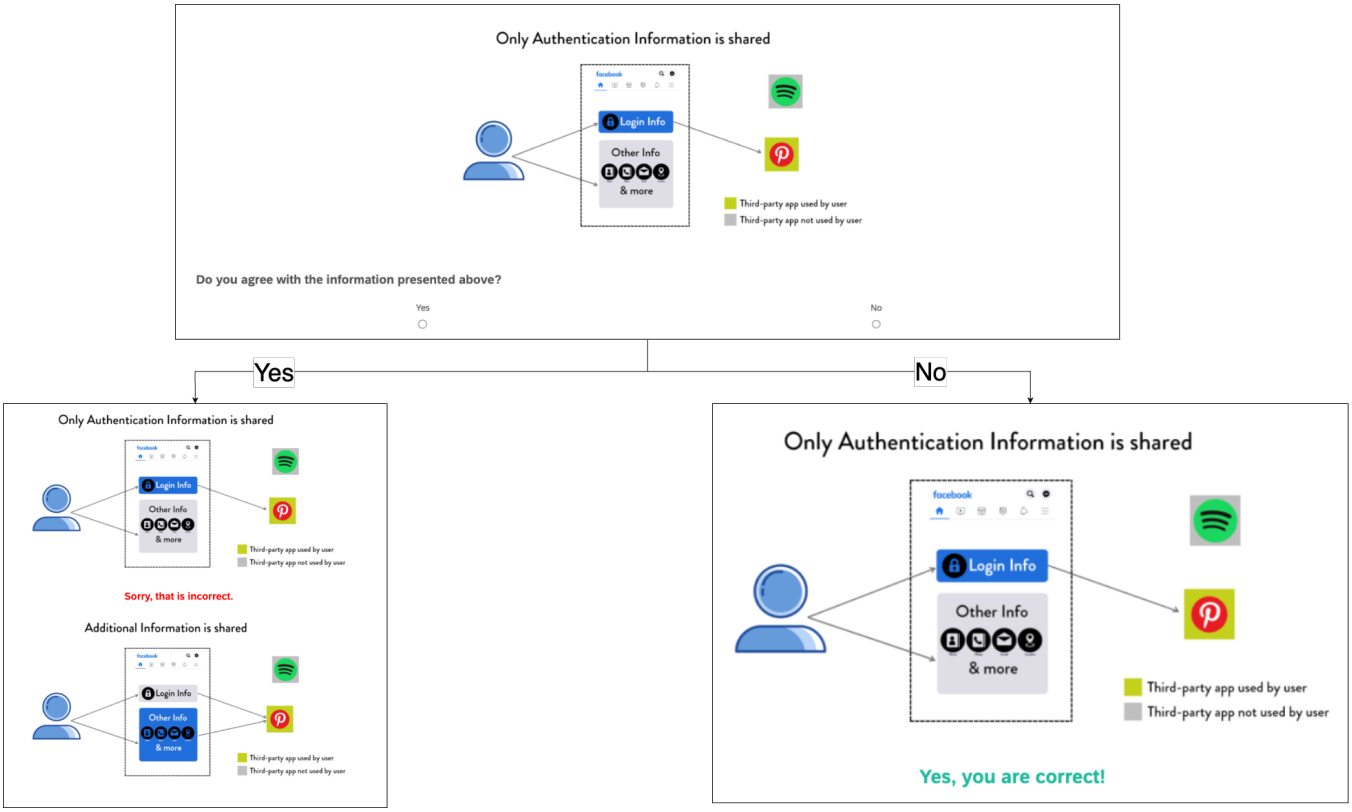
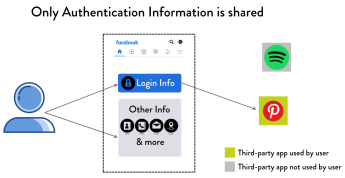
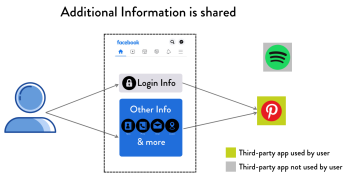


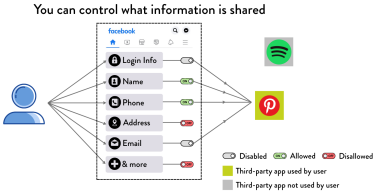
Figure 4: Online Study: Flow of the Design



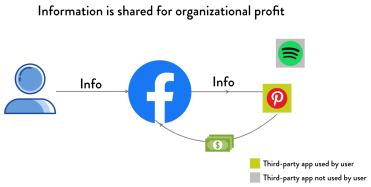
(a) Single Sign-On



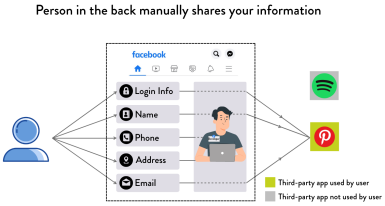
(b) Additional Sharing



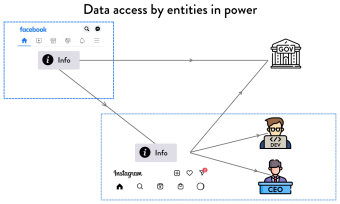
(c) Data Control



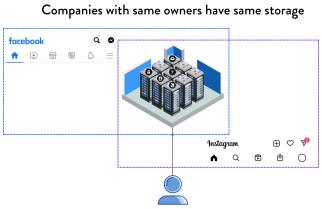
(d) Organizational Profit



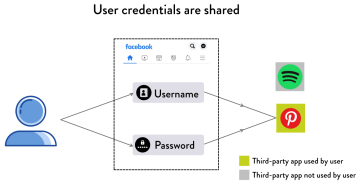
(e) Person in the Back



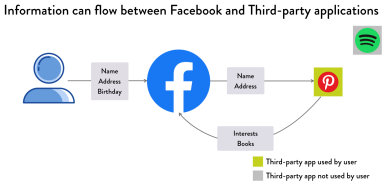
(f) Powerful Entities



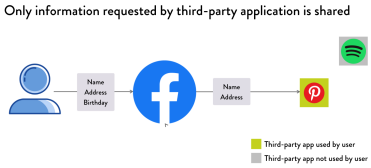
(g) Shared Ownership



(h) Credential Sharing



(i) Bidirectional Data Flow



(j) Partial Sharing

Figure 5: Treatment Conditions: Mental Model based Designs