Usable privacy

from grounded models to new guidelines and heuristics

André de Lima Salgado
andre.salgado@ufla.br
University of São Paulo and Universidade Federal de Lavras
Lavras, MG, Brazil

Renata Pontin de Mattos Fortes
renata@icmc.usp.br
University of São Paulo
São Carlos, SP, Brazil, renata@icmc.usp.br

Abstract

The development of usable interfaces for privacy policies is essential to increase users' trust in technology and comply with legal requirements. This thesis aimed to design interfaces that allow laypeople to protect their online privacy. A comprehensive analysis was conducted, comprising a literature review, a thematic and cluster analysis, and an empirical evaluation. Six usable privacy heuristics (push) were derived, which effectively detect severe problems in privacy policy interfaces for laypeople. Moreover, initial usable privacy guidelines (pug) were formulated, and a novel process for developing usability criteria was proposed. Future research directions were suggested, such as applying these heuristics and guidelines to domains like human-robot interaction and human-artificial intelligence interaction.

Keywords: usable privacy, heuristic, heuristic evaluation, usability, inspection, security

1 Introduction

Governments worldwide have introduced privacy legislation, such as the European Union General Data Protection Act (GDPR), the California Consumer Privacy Act (CCPA), the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), the Japanese Act on Protection of Personal Information (APPI), and the Brazilian General Personal Data Protection Law (LGPD) [32]. These regulations emphasize the need for individuals and organizations to obtain appropriate authorization before handling personal data. In the context of information technology, this implies that users must be informed and given the freedom to decide whether to share their personal information with other entities [32].

To inform users about data collection and usage, information technology companies commonly present privacy policies within their software applications [1, 32]. These policies often include privacy choices and settings that allow users to determine how their personal data is shared [15, 17, 33]. However, privacy policy interfaces tend to be complex and lack usability [2, 7, 17, 25, 26], increasing the risk of human error and associated threats to companies' information security [24]. Furthermore, designing usable privacy policy interfaces is crucial for achieving transparency, as mandated by privacy regulations [17].

This research aims to address the existing gap in the literature by developing usability heuristics specifically tailored for privacy policy interfaces targeting non-experts. While numerous usability heuristics can be found in the literature [8, 12, 18], there is a notable lack of heuristics focusing on privacy policy interfaces for laypeople. This gap hinders the integration of usability evaluation and information security in the context of privacy. Therefore, the objective of this study is to fill this void. The remainder of this paper describes methods and results related to the core of this Ph.D. research. Nevertheless, we point out additional contributions at Section 4.

2 Usable Privacy and Security

Regarding privacy and security, software can be deemed usable when its users are reliably informed about the necessary security tasks they must undertake, capable of successfully executing these tasks, avoid critical errors, and feel sufficiently at ease with the interface to sustain usage [38, p. 2].

A series of global standards [19, 20] acknowledge usability as a component of software quality and ergonomic design. These standards delineate usability through the concepts of the *user*, *goal*, *effectiveness*, *efficiency*, *satisfaction*, *context of use*, and *task*. According to these standards, usability is characterized as:

> "*the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use*"

The domain of Usable Privacy and Security (UPS) is dedicated to investigating the usability of systems designed to assist end-users or administrators in managing security and privacy concerns [7, 15]. Over the last two decades, the UPS field has experienced rapid growth [6, 7, 15, 34]. Initially, the relationship between usability and security was often viewed as contradictory, with users being perceived as the

In: V Concurso de Teses e Dissertações (CTD 2023), Ribeirão Preto, Brasil. Anais Estendidos do Simpósio Brasileiro de Sistemas Multimídia e Web (WebMedia). Porto Alegre: Sociedade Brasileira de Computação, 2023.

ISSN 2596-1683

primary threat to information security [34]. However, as the spectrum of potential threats expanded due to the ubiquity of data [2], everyday individuals were increasingly tasked with making security decisions [22], and they emerged as a pivotal factor in the field's advancement [34]. It became evident that even experts could inadvertently misconfigure systems and leave vulnerabilities without user-friendly tools [31]. Consequently, blame for security breaches might shift from users to designers [37]. Despite this evolution, certain fundamental aspects of how laypeople interact with privacy tools, such as mental models [25], remain underexplored in the literature. The UPS field continues to require user-friendly tools tailored for laypeople [2], along with suitable usability methodologies catered to this specific domain.

Examples of prominent themes within the UPS domain encompass, but are not confined to, social media privacy, user authentication, anti-phishing endeavors, Web privacy, and equitable information practices. This research endeavor centers on Web privacy and equitable information practices, concentrating on the challenges associated with crafting privacy policy tools that are user-friendly for individuals without specialized knowledge. The impetus behind addressing Web privacy and equitable information practices arises from the escalating opportunities for data collection facilitated by the Internet. Online retailers, in particular, gained unprecedented capabilities to amass and scrutinize data pertaining to their clientele [15]. Consequently, privacy regulations stipulate that users must possess awareness and agency in deciding whether to share their personal information with external entities [32]. To this end, the U.S. Government mandated companies to safeguard users' privacy through disclosure and choice mechanisms [15]. Similarly, the General Data Protection Regulation (GDPR) compelled enterprises within the European Union to empower individuals with control over their data sharing activities on the Web [35]. Notably, the Brazilian Government also upholds Web users' privacy rights [1]. Subsequent sections delve into the usability aspects of privacy policy tools.

Parallel to usability, information security is deeply intertwined with industry benchmarks. While defining usability remains a challenge in scholarly discourse, defining information security frequently revolves around upholding the confidentiality, availability, and integrity of information. As technology advances, new attributes may augment these core aspects to better address the intricacies of information security processes [36]. Consequently, it is reasonable to conceive of the term "usable security" as the endeavor to render the information security process user-friendly. However, it is important to acknowledge that this perspective doesn't encompass the entirety of the usable privacy and security domain.

If usable security is to design usable security processes, we should assume that users' goal is to secure the system. But, "security is usually a secondary goal" for laypeople [38]. The unmotivated user property, as defined by Whitten and Tygar [38], states that:

> Security is usually a secondary goal. People do not generally sit down at their computers wanting to manage their security; rather, they want to send an email, browse web pages, or download software, and they want security in place to protect them while they do those things. It is easy for people to put off learning about security, or to optimistically assume that their security is working, while they focus on their primary goals. Designers of user interfaces for security should not assume that users will be motivated to read manuals or to go looking for security controls that are designed to be unobtrusive. Furthermore, if security is too difficult or annoying, users may give up on it altogether.

This thesis delves into an exploration of the usability of privacy policy interfaces tailored for individuals without technical expertise, specifically targeting the safeguarding of children's privacy, termed as parental privacy control. The underlying premise is that the desire to manage the privacy of their loved ones serves as a motivational factor encouraging laypeople to engage with privacy policy interfaces.

Commonly, privacy policy tools encompass a combination of interfaces and mechanisms for policy creation, comprehension, configuration (referred to as privacy choice), and feedback provision. These mechanisms encapsulate the primary components of privacy policy tools [26]. As outlined by Paci et al. [26], a significant portion of research pertaining to policy creation centers around automated or semi-automated policy generation methods. Studies concerning policy comprehension frequently introduce novel interface designs, a strategy mirrored in endeavors aimed at enhancing policy comprehension interfaces. Conversely, investigations into feedback generation primarily revolve around furnishing feedback pertinent to access decision-making [26]. This work concentrates on research related to privacy policy comprehension and configuration/choice, given that within the literature, these studies predominantly introduce fresh interface designs for this domain.

3 Methods and Results

To develop the usability heuristics, we performed a thematic analysis of 45 transcripts retrieved from the literature, associating them with higher-level themes [3, 5]. These transcripts consist of user feedback and provide empirical indications of user behavior with privacy policy tools. Two researchers independently coded the initial themes by identifying user

[1] Federal Law Number 12.965 (2014): http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L12965.htm

behaviors in the transcripts, continuing the process until theoretical saturation was reached. A total of 19 initial themes were identified, representing the main usability issues encountered by laypeople when interacting with privacy policy tools. These themes were then revised to suggest usable privacy recommendations for future designs of privacy policy tools. The resulting recommendations serve as design requirements for the development of privacy policy tools and can be seen as a preliminary set of "Privacy and Usability Guidelines (pug's)".

After achieving saturation of the initial themes, we revisited the 45 transcripts to record the occurrences of the 19 initial themes. A cluster analysis was then conducted on this dataset to identify higher-level themes that could form the basis of the new heuristics. The 19 privacy and usability guidelines (pug's) were used as objects in the cluster analysis, with their occurrences serving as attributes. Ward's method and Jaccard's distance were applied to cluster the objects, aiming to minimize within-group dispersion and avoid weighting negative matches. A maximum of ten clusters was sought to correspond to a maximum of ten heuristics, ensuring a clear distinction from usability guidelines. Ultimately, six clusters were identified, forming the basis of the developed usable privacy heuristics, referred to as "Privacy and Usability Heuristics (push)". These heuristics were numbered from 1 to 6 based on their explanatory power within the data. Heuristics with higher explanatory power were listed first. The six usable privacy heuristics, which we call *Privacy and Usability Heuristics (push#)* are:

push#1 Readability of privacy policies.
The readability of privacy policies is crucial for users to understand how they share their data. Users may want to access personalized privacy analysis to understand the risks of sharing their data. While users set their privacy choices, they become vigilant and start to explore the interface and assess policies. They may also prefer interfaces with fewer privacy choices instead of complex settings.

push#2 Users' doubt and precaution.
Users may assess the consequences of others' privacy choices before deciding about sharing their own.

push#3 Provide help and avoid jargon.
Users may search for specific information, such as terms and definitions, or seek help to understand privacy policies. Avoid jargon.

push#4 Discretionary access control.
Users may want to know the extent to which their personal data is being shared. They may also want to know who accesses their personal data. After that, they may want to restrict access to their data.

push#5 Fast interaction and human error vulnerabilities.
Users may seek fast interactions with privacy policies. To this end, they deduce how the interface works. In these cases, they need to quickly understand how the privacy choice settings work (conceptual model), and human error is very likely to occur.

push#6 Unstable choices and appropriate symbols.
Users may change their privacy choices over time. A good policy-choice mapping is desirable in these situations. Employing appropriate symbols enhances the mapping.

To evaluate the effectiveness of the push# heuristics for privacy controls, a quasi-experimental study with a between-group design was conducted, comparing these new heuristics against the state-of-the-art usability heuristics proposed by Jaferian et al. [8, 21]. Start-up professionals were invited to participate voluntarily in the study, and they were randomly assigned to either the control group (using Jaferian et al.'s heuristics) or the treatment group (using the push# heuristics). The sample size for each group was determined following the recommendations of Caine [4], aiming for statistical power with Cohen's $d = 0.5$, $\alpha = 0.05$, and $\beta = 0.85$. Based on these requirements, a minimum of four participants in each group was required. The evaluation focused on the parental privacy control model proposed by Rafferty et al. [27], which was prototyped and accessed online via a browser simulation of a mobile device. The performance of the heuristics was compared based on the downstream utility, a measure of their ability to generate valuable outputs for the design change process. Usability problems identified by participants were categorized according to their severity using a scale proposed by Yankson et al. [39], with a focus on privacy-related issues.

Downstream utility on catastrophic problems

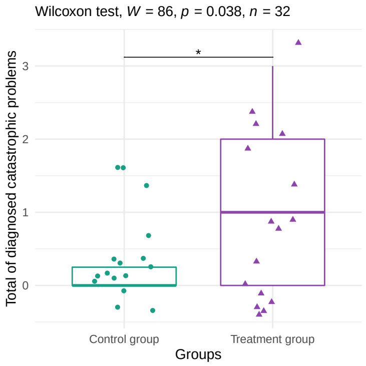
We compared the downstream utility on the number of catastrophic problems diagnosed by participants in each group. In the control group, participants discovered a minimum of zero and a maximum of two catastrophic usability problems ($\bar{X} = 0.375, M = 0.00, S \approx 0.72$). Meanwhile, in the treatment group, participants discovered a minimum of zero and a maximum of three catastrophic usability problems ($\bar{X} = 0.9375, M = 1.00, S \approx 1.00$). After a normality test, both the results' distribution from the control group ($p - value = 9.986e - 06$) and from the treatment group ($p - value \approx 0.0065$) significantly differed from a normal distribution. Therefore, as indicated by Lazar et al. [23], we employed the Wilcoxon signed-rank test to statistically compare the downstream utility of the number of catastrophic problems between groups. The results are shown in Figure 1 with jitter, boxplots, and the respective statistical results. For the downstream utility on catastrophic problems, evaluators' performance using the push# heuristics was significantly greater than the performance of evaluators using the state-of-the-art ($p - value = 0.038$). In addition, the data analysis showed a moderate effect size (0.317).

For instance, the results of push# heuristics' performance on catastrophic problems evidence its benefits over the state-of-the-art. For this reason, we accept the thesis hypothesis for the scope of catastrophic problems.

Downstream utility on major problems

Comparing the downstream utility on the number of major problems reported, participants in the control group discovered a minimum of zero and a maximum of four major

Figure 1. Results of the Wilcoxon signed-rank test.



problems ($\bar{X} = 1.00, M = 0.00, S \approx 1.37$). Meanwhile, in the treatment group, participants discovered a minimum of zero and a maximum of six major problems ($\bar{X} = 1.562, M = 1.50, S \approx 1.82$). After a normality test, both results' distribution from the control ($p - value \approx 0.0008$) and treatment ($p - value \approx 0.004$) group significantly differed from a normal distribution. Therefore, we compared the number of diagnosed problems between groups by applying the Wilcoxon signed-rank test. Although the observed results from the treatment group suggest a slight improvement compared with the control group, both groups had similar performance in this measure.

Overall number of usability problems reported

In addition to comparing the downstream utility of the heuristics, we compared the number of usability problems diagnosed by participants in each group. In the control group, participants discovered a minimum of zero and a maximum of five usability problems ($\bar{X} = 1.75, M = 1.00, S \approx 1.95$). Meanwhile, in the treatment group, participants discovered a minimum of zero and a maximum of eight usability problems ($\bar{X} = 3.125, M = 3.00, S \approx 2.66$). After a normality test, the results' distribution from the control group significantly differed from a normal distribution ($p - value \approx 0.002$), while the results' distribution from the treatment group did not ($p - value \approx 0.14$). Therefore, we compared the number of diagnosed problems between groups by applying the Wilcoxon signed-rank test. Although the results from the treatment group suggest an overall improvement compared with the control group, the difference was not significant.

Number of minor and cosmetic problems reported

Comparing the number of minor problems reported, participants in the control group discovered a minimum of zero and a maximum of one minor problem ($\bar{X} = 0.375, M = 0.00, S = 0.5$). Meanwhile, in the treatment group, participants discovered a minimum of zero and a maximum of two minor problems ($\bar{X} = 0.375, M = 0.00, S \approx 0.62$). After a normality test, both results' distribution from the control ($p - value = 2.566e - 05$) and treatment ($p - value = 4.803e - 05$) group significantly differed from a normal distribution. Therefore, we compared the number of diagnosed problems between groups by applying the Wilcoxon signed-rank test. Although the treatment group's observed results suggest a slight improvement compared with the control group, both groups had similar performance in this measure.

Similar to the number of minor problems, we observed a slight difference in the number of cosmetic problems reported between groups. Participants in the control group did not find any cosmetic problems. Meanwhile, in the treatment group, participants discovered a minimum of zero and a maximum of three cosmetic problems ($\bar{X} = 0.25, M = 0.00, S \approx 0.77$). After a normality test, the results' distribution from the treatment group did not ($p - value = 2.444e - 07$).

The data analysis on the discovery of cosmetic problems suggests that the push# heuristics have higher coverage over the ITSM. However, the observed results are not significant to confirm it.

4 Conclusions and Contributions

This doctoral research began with exploratory studies in game and web accessibility, usability inspection for novice evaluators, and methods for comparing usability finding reports [9, 13, 16, 29]. These studies emphasized the importance of supporting software development teams with context information to improve user interface evaluation outcomes and highlighted the challenges of comparing usability findings.

Thereafter, state-of-the-art usability heuristics were identified for evaluating privacy policy interfaces [8]. Pilot studies and experiments were conducted to create usable privacy recommendations, assess user behavior in the privacy context, and pilot methodology [10, 11, 14, 30]. The results provided valuable insights and contributed to the creation of usability criteria and guidelines.

In the second iteration of the PhD planning stage, users' behavior with privacy protection interfaces was further explored, including studies on smart toys, Data Glove interfaces, and connected-autonomous vehicles [10, 14, 30]. Our usability criteria creation method was piloted using grounded theory techniques [11]. Also, we revisited the severity rating criteria for usability problems found on privacy policy control applications [39].

In the final executing stage, new usable privacy criteria were created and evaluated, focusing on parental privacy control interfaces of smart toys. Overall, this doctoral research delivered nine papers and one book section to the literature as is. Besides, it also generated one registered software.

The comprehensive and extended version of this paper can be found in the referenced study by Salgado et al. [28]. This extensive rendition delves deeper into the research presented in the initial paper, providing a more intricate analysis, additional experimental results, and an enriched discussion of the findings. Readers interested in gaining a more comprehensive understanding of the subject matter are encouraged to refer to this extended version, which offers a more comprehensive and detailed exploration of the concepts and insights originally introduced.

Acknowledgments

This study was supported by the grants 2017/ 15239-0 and 2018/26038-8, São Paulo Research Foundation (FAPESP). This study was funded in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001.

References

[1] Esma Aïmeur, Oluwa Lawani, and Kimiz Dalkir. 2016. When changing the look of privacy policies affects user trust: An experimental study. *Computers in Human Behavior* 58 (May 2016), 368–379. https://doi.org/10.1016/j.chb.2015.11.014

[2] E. Bertino. 2016. Data Security and Privacy: Concepts, Approaches, and Research Directions. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 1. 400–407. https://doi.org/10.1109/COMPSAC.2016.89

[3] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (Jan. 2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[4] Kelly Caine. 2016. Local Standards for Sample Size at CHI. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 981–992. https://doi.org/10.1145/2858036.2858498

[5] Victoria Clarke and Virginia Braun. 2014. Thematic Analysis. In *Encyclopedia of Critical Psychology*, Thomas Teo (Ed.). Springer New York, New York, NY, 1947–1952. https://doi.org/10.1007/978-1-4614-5583-7_311

[6] L. F. Cranor and N. Buchler. 2014. Better Together: Usability and Security Go Hand in Hand. *IEEE Security Privacy* 12, 6 (Nov. 2014), 89–93. https://doi.org/10.1109/MSP.2014.109

[7] Luca Alexander De and Emanuel von Zezschwitz. 2016. Usable privacy and security. *it - Information Technology* 58, 5 (2016), 215–216. https://doi.org/10.1515/itit-2016-0034

[8] André de Lima Salgado, Renata Pontin de Mattos Fortes, Ricardo Ramos de Oliveira, and André Pimenta Freire. 2020. Usability heuristics on parental privacy controls for smart toys: From an exploratory map to a confirmatory research. *Electronic Commerce Research and Applications* 42 (2020), 100984. https://doi.org/10.1016/j.elerap.2020.100984

[9] André de Lima Salgado, Flávia de Souza Santos, Renata Pontin de Mattos Fortes, and Patrick C. K. Hung. 2018. Guiding Usability Newcomers to Understand the Context of Use: Towards Models of Collaborative Heuristic Evaluation. In *Behavior Engineering and Applications*, Raymond Wong, Chi-Hung Chi, and Patrick C. K. Hung (Eds.). Springer International Publishing, Cham, 149–168. https://doi.org/10.1007/978-3-319-76430-6_7

[10] André de Lima Salgado, Felipe Silva Dias, João Pedro Rodrigues Mattos, Renata Pontin de Mattos Fortes, and Patrick C. K. Hung. 2019. Smart toys and children's privacy: usable privacy policy insights from a card sorting experiment. In *Proceedings of the 37th ACM International Conference on the Design of Communication*. ACM, Portland Oregon, 1–8. https://doi.org/10.1145/3328020.3353951

[11] André de Lima Salgado, Fernanda Maciel Federici, Renata Pontin de Mattos Fortes, and Vivian Genaro Motti. 2019. Startup Workplace, Mobile Games, and Older Adults: A Practical Guide on UX, Usability, and Accessibility Evaluation. In *Proceedings of the 37th ACM International Conference on the Design of Communication* (Portland, Oregon) *(SIGDOC '19)*. Association for Computing Machinery, New York, NY, USA, Article 15, 9 pages. https://doi.org/10.1145/3328020.3353948

[12] André de Lima Salgado, Sandra Souza Rodrigues, and Renata Pontin M. Fortes. 2016. Evolving Heuristic Evaluation for Multiple Contexts and Audiences: Perspectives from a Mapping Study. In *Proceedings of the 34th ACM International Conference on the Design of Communication (SIGDOC '16)*. ACM, New York, NY, USA, 19:1–19:8. https://doi.org/10.1145/2987592.2987617

[13] Flávia de Souza Santos, André de Lima Salgado, and Renata Pontin de Mattos Fortes. 2018. Um Mapeamento Sistemático sobre Acessibilidade e Usabilidade no Desenvolvimento de Jogos Digitais para Idosos. *iSys-Brazilian Journal of Information Systems* 11, 2 (2018), 63–90.

[14] Matthew Demoe, Alvaro Uribe-Quevedo, André L. Salgado, Hidenori Mimura, Kamen Kanev, and Patrick C.K. Hung. 2020. Exploring Data Glove and Robotics Hand Exergaming: Lessons Learned. In *2020 IEEE 8th International Conference on Serious Games and Applications for Health (SeGAH)*. 1–8. https://doi.org/10.1109/SeGAH49190.2020.9201747

[15] Simson Garfinkel and Heather Richter Lipford. 2014. *Usable Security: History, Themes, and Challenges*. SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, AND TRUST, Vol. 5. Morgan & Claypool Publishers.

[16] Felipe Tassario Gomes, André de Lima Salgado, Lianna Mara Castro Duarte, Flávia de Souza Santos, and Renata Pontin Fortes. 2018. Um Simulador Visual de Leitor de Telas para Auxílio à Interpretação de Questões de Acessibilidade por Avaliadores Videntes. *Revista de Sistemas e Computação-RSC* 8, 1 (2018).

[17] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. "It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–12. https://doi.org/10.1145/3313831.3376511

[18] Setia Hermawati and Glyn Lawson. 2016. Establishing usability heuristics for heuristics evaluation in a specific domain: Is there a consensus? *Applied Ergonomics* 56 (2016), 34 – 51. https://doi.org/10.1016/j.apergo.2015.11.016

[19] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. 2010. Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems. www.iso.org/obp/ui/#iso:std:iso:9241:-210:ed-1:v1:en

[20] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. 2016. *ISO/IEC 25066:2016(en), Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for Usability — Evaluation Report*. Technical Report. https://www.iso.org/obp/ui/#iso:std:iso-iec:25066:ed-1:v1:en

[21] Pooya Jaferian, Kirstie Hawkey, Andreas Sotirakopoulos, Maria Velez-Rojas, and Konstantin Beznosov. 2014. Heuristics for Evaluating IT Security Management Tools. *Human–Computer Interaction* 29, 4 (July 2014), 311–350. https://doi.org/10.1080/07370024.2013.819198

[22] Julian Jang-Jaccard and Surya Nepal. 2014. A survey of emerging threats in cybersecurity. *J. Comput. System Sci.* 80, 5 (Aug. 2014), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

[23] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. *Research methods in human-computer interaction*. Morgan Kaufmann, Cambridge, MA, USA.

[24] Jan Meszaros and Alena Buchalcevova. 2017. Introducing OSSF: A framework for online service cybersecurity risk management. *Computers & Security* 65 (March 2017), 300–313. https://doi.org/10.1016/j.cose.2016.12.008

[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). https://content.sciendo.com/view/journals/popets/2018/4/article-p5.xml

[26] Federica Paci, Anna Squicciarini, and Nicola Zannone. 2018. Survey on Access Control for Community-Centered Collaborative Systems. *ACM Comput. Surv.* 51, 1 (Jan. 2018), 6:1–6:38. https://doi.org/10.1145/3146025

[27] Laura Rafferty, Marcelo Fantinato, and Patrick C. K. Hung. 2015. Privacy Requirements in Toy Computing. In *Mobile Services for Toy Computing*, Patrick C. K. Hung (Ed.). Springer International Publishing, 141–173. http://link.springer.com/chapter/10.1007/978-3-319-21323-1_8

[28] André de Lima Salgado, Patrick C. K. Hung, and Renata P. M. Fortes. 2023. Six usable privacy heuristics. In *Anais do XXII Simpósio Brasileiro de Informática na Educação*. SBC.

[29] André de Lima Salgado, Renata Pontin de Mattos Fortes, Patrick CK Hung, and Dilvan de Abreu Moreira. 2019. A Method for Classifying Usability Findings to Enhance Validation of New Heuristics. *Revista de Sistemas e Computação-RSC* 9, 1 (2019).

[30] André de Lima Salgado, Ben Singh, Patrick C. K. Hung, Annie Jiang, Yen-Hung Liu, Anna Priscilla de Albuquerque Wheler, and Hossam A. Gaber. 2020. Preliminary Tendencies of Users' Expectations about Privacy on Connected-Autonomous Vehicles. In *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. 296–301. https://doi.org/10.1109/SMC42975.2020.9282844

[31] M. A. Sasse and M. Smith. 2016. The Security-Usability Tradeoff Myth [Guest editors' introduction]. *IEEE Security Privacy* 14, 5 (Sept. 2016), 11–13. https://doi.org/10.1109/MSP.2016.102

[32] F. Schaub, R. Balebako, and L. F. Cranor. 2017. Designing Effective Privacy Notices and Controls. *IEEE Internet Computing* 21, 3 (May 2017), 70–77. https://doi.org/10.1109/MIC.2017.75

[33] Alec N Slepchuk and George R Milne. 2020. Informing the design of better privacy policies. *Current Opinion in Psychology* 31 (Feb. 2020), 89–93. https://doi.org/10.1016/j.copsyc.2019.08.007

[34] Jeremiah D. Still. 2016. Cybersecurity Needs You! *interactions* 23, 3 (April 2016), 54–58. https://doi.org/10.1145/2899383

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

[36] Rossouw von Solms and Johan van Niekerk. 2013. From information security to cyber security. *Computers & Security* 38 (2013), 97–102. https://doi.org/10.1016/j.cose.2013.04.004 Cybercrime in the Digital Economy.

[37] R. Wash and M. E. Zurko. 2017. Usable Security. *IEEE Internet Computing* 21, 3 (May 2017), 19–21. https://doi.org/10.1109/MIC.2017.69

[38] Alma Whitten and J. D. Tygar. 1999. Why Johnny Can'T Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8 (SSYM'99)*. USENIX Association, Berkeley, CA, USA, 14–14. http://dl.acm.org/citation.cfm?id=1251421.1251435

[39] Benjamin Yankson, Andre L Salgado, and Renata PM Fortes. 2021. Recommendations to Enhance Privacy and Usability of Smart Toys. In *Proceedings of the 54th Hawaii International Conference on System Sciences*. 1868.