



**Selected Papers of #AoIR2024:
The 25th Annual Conference of the
Association of Internet Researchers**
Sheffield, UK / 30 Oct - 2 Nov 2024

WHO HAS THE POWER?: A COMPARATIVE ANALYSIS OF PARENTAL CONTROLS ON SOCIAL MEDIA PLATFORMS

Chelsea L. Horne
American University

Introduction

One recent trend in social media platform practices as well as in proposed policy and regulation for online data rights is a turn towards parental controls. For example, in the United States, the 2023 Kids Online Safety Act (KOSA) is the first bill to specifically refer to “parental controls.” A few years earlier, the proposed 2020 DETOUR Act mentioned “parental consent,” but not controls specifically. There are also ongoing lawsuits in the US that claim faulty design on online platforms’ parental controls, thus leading to harm to children. While concerns over children’s safety online and complaints about problematic settings are not necessarily new (Horne, 2021; Horne, 2023b), there may be an emerging trend in some countries to try to address growing concerns about the impact of social media platforms by setting regulation on parental controls.

Privacy settings, default selections, and by extension parental controls have significant power to impact users’ privacy and overall experience on social media platforms. That said, the literature indicates that many people do not change their default privacy settings (Dinner et al., 2011; Ramokapane et al., 2019; Shah & Sandvig, 2008; Sunstein, 2013; Svirsky, 2019; Watson et al., 2015). Because “technical arrangements are arrangements of power” (DeNardis, 2014), it is of critical research importance to consider the design, structure, and practice of platform settings. To that end, more research is currently needed to study parental controls and age-specific settings for teens and children, as these are comparatively newer developments and a topic and platform feature in flux. This paper contributes to this needed research area by focusing on specific definitions and understandings of privacy.

The apparent appeal of parental controls is the ability of social media platforms to offer a visible space to exert “choice and control” to users’ parents (Freishtat & Sandlin, 2010; Hoffmann et al., 2018). On the other hand, the practice of relying on parental action as a key in protecting children online, places the burden of responsibility on the

Suggested Citation (APA): Horne, C. (2024, October). *Who Has the Power?: A Comparative Analysis of Parental Controls on Social Media Platforms*. Paper presented at AoIR2024: The 25th Annual Conference of the Association of Internet Researchers. Sheffield, UK: AoIR. Retrieved from <http://spir.aoir.org>.

parent, which may raise concerns about privacy literacy, information overload, and children's rights.

Methodology

The purpose of this study is two-fold. Many social media platforms offer both age-specific privacy settings to children under certain age, as well as parental controls to manage the account of their children. As a result, this study will examine which parental controls are available and how they are offered across some of the most popular social media platforms: Facebook, Instagram, TikTok, Discord, and YouTube. The average user has 8.5 social media accounts (Dixon, 2022), so a comparative approach to parental controls offers a comprehensive look at users' experiences.

The dataset for this study will consist of each social media platform's: 1. default settings of teen and children's accounts and 2. parental control options. The analysis will broadly consider how each platform defines parental controls via privacy options. Further questions include: What kinds of control choices are offered? How do these choices differ across platforms? These are significant questions because the design of platform choice architecture has the ability to influence online experiences. The research questions for this paper are:

1. What parental controls do different social media platforms offer?
2. What privacy topics do social media platforms' parental controls address?
3. Are social media platforms' default settings preset towards more restrictive choices (increased privacy) or towards more public choices (increased sharing)?

The first and second research questions consider if there are differences, and if so, what differences exist between controls options for each platform. The aim of the study is not to determine the "best" types of parental controls and design features, but to track the range of options in order to better understand the opportunities and challenges of relying on parental controls to manage children's privacy online and mitigate potential harms. The comparative approach captures the reality for children and parents as they likely will have to manage multiple social media platform accounts, that have vastly different options and privacy perspectives. Finally, the third research question considers the impact and positionality in default selections as these pre-set choices can significantly shape a child's experience online, especially since teens and children may not have the literacy skills to manage them by themselves.

In terms of methodology and analysis, this paper uses the typology of privacy settings to analyze the privacy topics of parental controls (Horne, 2023a). This typology offers a granular look at privacy in practice by operationalized seven discrete components of privacy: Visibility, Discoverability, Bounderability, Content, Account Security, Data Access/Portability, and Data Sharing/Personalization.

Conclusions

The findings indicate that much like overall privacy and standard privacy settings, parental controls are also “a concept in disarray” (Solove, 2008). The study found that parental controls emphasized three types of privacy: Discoverability, Bounderability, and Content. Across platforms, the quantity of choices as well as the types of choices varied significantly. In general though, parental controls are currently focused most on Bounderability options—choices that are aimed at setting limits for the child’s account. On the other hand, platforms take on most of the burden of Visibility type settings as these appear in the child/teen’s account via strong privacy default selections. This is of notable interest as it explains why Visibility settings are not apparent in parental controls: the platforms increase privacy themselves for children’s accounts. A final noteworthy finding is that the results indicate the emergence of a new type of setting that is discrete for parental controls: Transparency. Notably, Transparency parental controls only allow information from children’s account to be viewed, but not managed in any way.

References

- DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.
- Dinner, I., Johnson, E. J., Goldstein, D. G., & Liu, K. (2011). Partitioning default effects: Why people choose not to choose. *Journal of Experimental Psychology: Applied*, 17(4), 332–341. <https://doi.org/10.1037/a0024354>
- Dixon, S. (2022, April 28). *Global social media account ownership 2018*. Statista. <https://www.statista.com/statistics/788084/number-of-social-media-accounts/>
- Freishtat, R. L., & Sandlin, J. A. (2010). Shaping Youth Discourse About Technology: Technological Colonization, Manifest Destiny, and the Frontier Myth in Facebook’s Public Pedagogy. *Educational Studies*, 46(5), 503–523. <https://doi.org/10.1080/00131946.2010.510408>
- Hoffmann, A. L., Proferes, N., & Zimmer, M. (2018). “Making the world more open and connected”: Mark Zuckerberg and the discursive construction of Facebook and its users. *New Media & Society*, 20(1), 199–218. <https://doi.org/10.1177/1461444816660784>
- Horne, C. (2021). CHOICE AND CONTROL: AN ANALYSIS OF PRIVACY VALUES AND PRIVACY CONTROLS. *AoIR Selected Papers of Internet Research*. <https://doi.org/10.5210/spir.v2021i0.11944>
- Horne, C. L. (2023a). *In Settings We Trust: The Privacy Battle for Choice and Control*. 217. <https://doi.org/10.57912/25229699>
- Horne, C. L. (2023b). RULE BY DEFAULT: A CROSS-PLATFORM ANALYSIS OF PRIVACY SETTINGS. *AoIR Selected Papers of Internet Research*. <https://doi.org/10.5210/spir.v2022i0.13022>

- Ramokapane, K. M., Mazeli, A. C., & Rashid, A. (2019). Skip, Skip, Skip, Accept!!!: A Study on the Usability of Smartphone Manufacturer Provided Default Features and User Privacy. *Proceedings on Privacy Enhancing Technologies*, 2019(2), 209–227. <https://doi.org/10.2478/popets-2019-0027>
- Shah, R. C., & Sandvig, C. (2008). SOFTWARE DEFAULTS AS DE FACTO REGULATION The case of the wireless internet. *Information, Communication & Society*, 11(1), 25–46. <https://doi.org/10.1080/13691180701858836>
- Solove, D. J. (2008). *Understanding privacy / Daniel J. Solove*. Harvard University Press.
- Sunstein, C. R. (2013). Deciding by Default. *University of Pennsylvania Law Review*, 162(1), 1–58.
- Svirsky, D. (2019). Why do people avoid information about privacy? *Journal of Law & Innovation*, 2(1).
- Watson, J., Lipford, H. R., & Besmer, A. (2015). Mapping User Preference to Privacy Default Settings. *ACM Transactions on Computer-Human Interaction*, 22(6), 1–20. <https://doi.org/10.1145/2811257>