Selected Papers of #AoIR2022:
The 23rd Annual Conference of the
Association of Internet Researchers
Dublin, Ireland / 2-5 Nov 2022

RULE BY DEFAULT: A CROSS-PLATFORM ANALYSIS OF PRIVACY SETTINGS

Chelsea L. Horne
American University

Introduction

In 2018, the German court ruled that Facebook's use of personal data was illegal because Facebook "hi[d] default settings that are not privacy-friendly" and did not meet the overall requirement for informed consent (Busemann & Schimroszik, 2018). That same year, the Italian regulator fined Facebook 10 million euros in part because of a default setting that forced an "aggressive practice" by automatically preparing "transmission of user data to individual websites/apps without express consent" (Hern, 2018). In 2019, the United States Federal Trade Commission (FTC) slammed Facebook with a $5 billion civil penalty for violations of privacy practices, including default settings (Fair, 2019). And in 2021, the Italian regulator fined Facebook another 7 million euros for continuing to mislead users. These recent enforcements and penalties on deceptive and problematic privacy settings highlight the practical and policy significance of settings within the larger scope of privacy and data regulation.

Just as scholars study privacy policies, terms of service, and the technical infrastructure and architecture of digital platforms' privacy and security choices, privacy settings are critical in discussions of privacy and privacy rights. Privacy settings are a critical space of research; settings are uniquely positioned at the intersection between users and digital platforms and regulation, providing a visible privacy architecture—unlike backend privacy infrastructure and code—as well as an opportunity for users to interact with privacy choices—unlike terms of service and privacy policy documents which offer only all-or-nothing options (Horne, 2021). As Laura DeNardis demonstrates "technical arrangements are arrangements of power" (DeNardis, 2014). The literature shows that privacy settings have profound ability to influence users (Shah & Sandvig, 2008; Soh, 2019; Zuiderveen Borgesuis, 2015), but also that most users do not change settings (Dinner et al., 2011; Sunstein, 2013; Svirsky, 2019).

This paper examines the structural power relations and hierarchies inherent within privacy settings. We address the conference theme of decolonizing the internet through

Suggested Citation (APA): Horne, C., (2022, November). Rule By Default: A Cross-Platform Analysis of Privacy Settings. Paper presented at AoIR 2022: The 23rd Annual Conference of the Association of Internet Researchers. Dublin, Ireland: AoIR. Retrieved from http://spir.aoir.org.

a comprehensive analysis of privacy controls, a critical site of power for the “new colonising forces in the form of multinational tech giants who are re-fashioning the world in their own image” (#AoIR2022 CFP).

Critical Framework

Current models of privacy are based on a control paradigm, which promotes an understanding of privacy as having control over one’s information. Part of the challenge of protecting privacy is that privacy is a “concept in disarray” (Solove, 2008) and resists specificity. Efforts to distill a definition lead to “vague, overinclusive, and underinclusive rules” (Citron & Solove, 2021) and allows industry to tailor services that leave users vulnerable (Cohen, 2019). Another challenge is that conversations on privacy are framed as a matter of individual responsibility rather than a larger social good. Platforms benefit from this frame as they pass responsibility for privacy-friendly practices to users, who platforms know will likely not change their settings.

This paper applies a theoretical framework of science & technology studies (STS) to analyze the affordances of social media platforms’ privacy settings. Further, we apply Ian Bogost’s theory of procedural rhetoric to examine how platforms apply “the art of using processes persuasively” (Bogost, 2007). The theory argues that games, their rules, and process-based systems make claims about the way the world works and reinforce the ideologies of game makers. The interactive process of choice architecture in privacy settings also lends itself to the procedural rhetoric framework. Procedural rhetoric demonstrates that the parameters of technology settings are ideological in nature and that the affordances of digital technology may hide mechanisms of power. Further, as Bogost suggests, through procedural rhetoric, people learn about the way the world works. A potential implication then is that privacy settings go beyond reinforcing hegemonic viewpoints and insinuate to users that these viewpoints are normative.

Methodology

This paper conducts a comparison study of privacy settings across some of the most popular social media platforms: Facebook, YouTube, Instagram, TikTok, and Twitter. Both the desktop and mobile version of each social media will be analyzed as the literature indicates that there may be differences between desktop and mobile versions, with the mobile versions more likely to have deceptive practices (Luguri & Strahilevitz, 2021). The purpose of this analysis is to examine how privacy is presented to users. How does each platform define privacy? Where do they locate different kinds of privacy settings? What kinds of privacy choices are offered? How do these choices differ? How a platform designs their choice architecture for privacy shapes a user’s understanding of what privacy is and means.

Conclusions

Users have long had to navigate dodgy defaults, sticky settings, and deceptive data practices and despite regulatory actions and new policies, the problems and privacy harms persist. As billions of people use social media to communicate with each other,

share information, read the news, and even access the internet, the decisions of technology companies on issues of privacy and security have global impacts.

This paper contributes to the larger conversation of privacy online through a comprehensive consideration of privacy settings, one key site where users and platforms both engage with privacy. Further, this study addresses the burden of individual responsibility to manage privacy online. Additionally, while more research is needed, it is possible that deceptive practices and non-privacy friendly settings may disproportionately affective members of marginalized communities (Benjamin, 2019; Shah & Sandvig, 2008). This project's cross-platform analysis of privacy settings also offers a new lens through which to analyze privacy settings and their implications. These findings could help scholars and policymakers understand how platforms deploy privacy choices and what ideologies regarding privacy they reify. It would also shed insight into the similar or conflicting definitions of privacy online that users must navigate via privacy settings.

References

Benjamin, R. (2019). Default Discrimination. In *Race After Technology*.

Bogost, I. (2007). *Persuasive Games: The Expressive Power of Videogames*. MIT Press.

Bradshaw, S., & DeNardis, L. (2019). Privacy by Infrastructure: The Unresolved Case of the Domain Name System: Privacy by Infrastructure. *Policy & Internet*, *11*(1), 16–36. https://doi.org/10.1002/poi3.195

Busemann, H.-E., & Schimroszik, N. (2018, February 12). German court rules Facebook use of personal data illegal. *Reuters*. https://www.reuters.com/article/us-germany-facebook-idUSKBN1FW1FI

Citron, D. K., & Solove, D. J. (2021). *Privacy Harms* (SSRN Scholarly Paper ID 3782222). Social Science Research Network. https://doi.org/10.2139/ssrn.3782222

Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism / Julie E. Cohen.* Oxford University Press.

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

Fair, L. (2019, July 24). *FTC's $5 billion Facebook settlement: Record-breaking and history-making*. Federal Trade Commission. https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history

Hern, A. (2018, December 7). Italian regulator fines Facebook £8.9m for misleading users. *The Guardian*. https://www.theguardian.com/technology/2018/dec/07/italian-regulator-fines-facebook-89m-for-misleading-users

Horne, C. L. (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

Luguri, J., & Strahilevitz, J. (2021). Shining a Light on Dark Patterns. *Journal of Legal Analysis*, *13*(1), 43–109. https://doi.org/doi.org/10.1093/jla/laaa006

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., & Kesan, J. P. (2008). SETTING ONLINE POLICY WITH SOFTWARE DEFAULTS. *Information, Communication & Society*, *11*(7), 989–1007. https://doi.org/10.1080/13691180802109097

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

Soh, S. Y. (2019). Privacy Nudges: *European Data Protection Law Review*, *5*(1), 65–74. https://doi.org/10.21552/edpl/2019/1/10

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

Willis, L. E. (2013). Why Not Privacy by Default? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2349766

Zuiderveen Borgesuis, F. (2015). *Nudge and the Law: A European Perspective* (A. Alemanno & Sibony, Eds.). Hart Publishing. https://doi.org/10.5040/9781474203463