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 “hid 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
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 affect 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


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


https://doi.org/10.2139/ssrn.2349766


https://doi.org/10.5040/9781474203463