Dark Patterns and Privacy Harms:
Accountability and Agency in an Age of Disappearing Privacy

Chelsea L. Horne
American University

Introduction

In 2019, the United States Federal Trade Commission (FTC) slammed Facebook with a record-breaking $5 billion civil penalty for violations of a previous FTC order on privacy practices (Fair, 2019). This penalty is significant not because of the amount, though it is twenty times higher than any previous U.S. fine, but because the FTC's decision may mark the solidification of a global paradigm shift. While scholars have long been wary about the largely unchecked, unregulated power of technology companies with increasing concerns about how users' data and privacy are managed, it is only in recent years that meaningful attention and accountability of tech companies has emerged. Additionally, from a societal perspective, trust in technology companies has tanked (Fried & Allen, 2021).

For many years, platforms and other tech companies have had significant, unregulated power to influence and control user experience. Especially since the the 2018 Cambridge Analytica revelations, there has been a profound push for more accountability of the online harms created and/or amplified by social media platforms. This "techlash" has primarily focused on issues of data privacy, privacy rights, content moderation, and cybersecurity. Current efforts in law and policy indicate this shift away from the unregulated power of the big tech industry towards greater user protection. The European Union's General Data Protection Regulation (GDPR) notably requires "data protection by design and by default" and is a prime example of how important default standards, settings, and protocols are in internet governance and regulation. Since then, further updates to data and privacy protection include the 2020 introduction of the Digital Services Acts and Digital Markets Acts, which more concretely outline new rules for digital service providers. In the US, a patchwork of privacy laws remains, though California and Illinois made notable steps towards enhanced data and privacy protection through the respective 2020 California Consumer Privacy Act (CCPA) and 2008 Biometric Information Privacy Act (BIPA). In recent years, the number of lawsuits, penalties, and settlements against technology companies for privacy violations has increased.

In an era where "privacy and anonymity may effectively disappear by choice or government mandate, as all aspects of personal and professional lives are tracked by global networks," the stakes for user-citizens are high (National Intelligence Council, 2021). With the rise of platforms and surveillance capitalism, the line between what is public and what is private has become convoluted (Zuboff, 2020). Lina Dencik and Jonathan Cable (Dencik & Cable, 2017) describe these normative infrastructures of surveillance as surveillance realism which "comes to regulate thought and action, in which the active normalization of surveillance infrastructures limits the possibilities of even imagining alternatives."

Perhaps most concerning in the battle over privacy is what Elinor Carmi calls the myth of the empowered user (Carmi, 2021). In a scathing rebuttal of Facebook's Vice President of Global Affairs Nick Clegg's (Clegg, 2021) claim that it "takes two to tango" and that users are active, enabled agents in their experiences online, Carmi points out the growing scholarship that empirically shows how users are constantly bombarded with deceptive user interface and design aimed at influencing user choices. In short, the perception and the reality of user agency online is fraught with tension and contradiction.

Today, we are at a critical juncture where privacy research can translate into policy action. This paper considers the evolution of privacy online through the lens of privacy and data controls. These user controls—also referred interchangeably as settings—offer insight into what choices companies provide to users. Further, this paper argues that the ways technology companies change, update, and set privacy controls reflect evolving expectations of privacy online as well companies' responses to regulatory action. To this end, this project tracks changes to privacy controls over the years and analyzes the privacy and data choices offered, their presentation to users, and the social and legal contexts that prompted these changes.

Literature Review

A unique opportunity to study privacy rests in user controls—how they are designed, their rhetorical deployment, and user interaction—as these settings help shape a user's security, privacy, and overall experience. Wendy Chun shows the taken-for-granted ideological and political power that software and its default settings—which she notes are ironically referred to as "your" preferences—slide between modes of (in)visibility (Chun, 2006). This paper focuses on privacy online with a particular focus on social media platform settings as a point of control between user and company. Perhaps most importantly, user controls offer the possibility for users to exert a level of agency in curating their online experience. Notably, the settings page is one of the only places where users have control over their online experience beyond opting out of the service entirely. And yet, despite this gilt of agency, these settings often reify hegemonic power structures. Ultimately, the larger picture of this project considers the social, economic, and legal contexts that establish the privacy controls that help shape our digital lives and further, to reflect on the implications for internet governance and potential regulatory options.

Rebecca MacKinnon suggests that platforms take a "Hobbesian approach to governance," where users engage in a Faustian-like exchange of their rights for use of services (MacKinnon, 2013). The Internet is a core network that influences the other networks in our lives. The result is that Internet-related companies have become incredibly powerful because they not only provide, but shape (through policies and enforcement) the digital spaces upon which citizens increasingly depend (MacKinnon, 2013). Digital platforms, services, and devices are a key component and mediate relationships of all kinds, including the relationship between citizens and government. Tarleton Gillespie suggests that content providers carefully frame themselves as "platforms," a strategic rhetorical flourish that offers flexibility and "suggests a progressive and egalitarian arrangement, promising to support those who stand upon it" (Gillespie, 2010). Moreover, this framing as an all-encompassing architectural, figurative, political, computational "platform" aids these companies' efforts to influence regulatory policy and economic interests (Gillespie, 2010). In later work, Gillespie (2018) expands on content providers' role and dubs these platforms the "custodians of the internet."

The policies, infrastructure, algorithms, and design of platforms have immense power. Laura DeNardis and Andrea Hackl contend that "social media platform policies and technical design serve as a form of *privatized governance* directly enacting rights and regulating the flow of information online" (DeNardis & Hackl, 2015). The privatization of internet governance and of human rights is of urgent concern as governments and users attempt to hold platforms accountable and the war over data rights continues. As one example, Siva Vaidhyanathan points out that the problem with Facebook is Facebook. Platforms have an information shaping function and are currently under little economic or regulatory motivation to address the issue (Vaidhyanathan, 2018). In fact, Vaidhyanathan argues that Facebook operates better when people are angry and hateful—meaning users are more likely to engage on the site—and so, if anything, these companies are financially motivated to maintain the status quo.

Of particular interest to this project is a consideration of the largely hidden power of privacy controls. The literature largely agrees and focuses on two key points regarding privacy controls and political implications. First, research on the role of default settings—those settings pre-set by companies—indicates the ability of defaults to influence human behavior, both in the analog and digital world (Bradshaw & DeNardis, 2019; Shah & Kesan, 2008; Shah & Sandvig, 2008; Soh, 2019; Willis, 2013; Zuiderveen Borgesuis, 2015). Second, research shows that most users do not change the default settings (Dinner et al., 2011; Ramokapane et al., 2019; Shah & Sandvig, 2008; Sunstein, 2013; Svirsky, 2019; Watson et al., 2015). These points together suggest that there is incredible and inherent—though hidden—power in privacy controls, including those set by online platforms. A default rule offers freedom of choice and does not inherently impose a choice on people, and instead "nudges" people in a direction, which in practice could be changed by the user if they wanted (Sunstein, 2013). And yet, Sunstein also acknowledges that defaults have incredible impact; defaults tend to be "sticky" and remain unchanged because people tend to ignore them.

Attention to the role of default selections has also underscored researchers work on bias and technology. Ruha Benjamin considers how digital architecture constructs and reflects bias in her concept of default discrimination, which is an element of her concept of The New Jim Code (Benjamin, 2019). Benjamin points out that the effects of discriminatory design are long-lasting and long-reaching and that "Collateral damage, we might say, is part and parcel of discriminatory design." Additionally, Caroline Criado-Perez examines data bias through the lens of gender and argues that with the assumption of the default male leads to the erasure and invisibility of women (Criado-Perez, 2019).

The hidden levers of control embedded within the privacy controls influence users' overall experience on platforms and with technology, especially regarding issues of privacy, data, and security. In other words, because users often do not change default settings, the decisions of technology companies serve to frame most users' experience online. Further research could indicate if default selections may do more than affect user for each respective technology, but also have implications on normative perceptions of major issues, such as privacy.

There is also growing concern about how platforms may be engaging in "dark patterns." Harry Brignull is credited with coining the term "dark patterns" in 2010 to describe the "tricks used in websites and apps that make you do things that you didn't mean to" (*Dark Patterns*). He also maintains the website darkpatterns.org, which is a popular website geared at documenting dark patterns and informing the public. Behavioral economists consider dark patterns to be a kind of "sludge" (Sunstein, 2019) and legal scholars may refer to them as market manipulation (Calo, 2013). These deceptive user interface designs are common and effective in influencing user behavior. For example, one study found evidence of dark patterns on 95% of free Android apps within their sample (Di Geronimo et al., 2020). Elinor Carmi also covers the effects of social media companies practices, and in particular default selections, as a way to engineer sociality (Carmi, 2020).

The literature on dark patterns is still emerging. One focus is determining definitions and understanding of what and how dark patterns function. A critical step identified the phenomenon of dark patterns and established a typology (Bösch et al., 2016; Gray et al., 2018). Of particular interest to this project are two types of dark patterns: 1. Privacy Zuckering which Tim Jones of the Electronic Frontier Foundation (EFF) described as "deliberately confusing jargon and user-interfaces" and Bösch et al. reconsidered as a universal privacy dark pattern and 2. Bad Defaults are those options pre-set by applications, websites, and social media companies that ease or encourage the sharing of personal information, and so cause users to unknowingly share more information than they may have wanted to (Bösch et al., 2016).

Scholarship has now turned to studying the effects and effectiveness of dark patterns. In what the study's authors claim is the first public evidence of the power of dark patterns, they discovered that users exposed to mild dark patterns were twice as likely to be influenced and users exposed to aggressive dark patterns were four times as likely (Luguri & Strahilevitz, 2021). Also of note, the study found that aggressive dark patterns received significant backlash, whereas mild patterns did not (Luguri & Strahilevitz, 2021). Again, while the larger phenomenon of deceptive interface is not necessarily new, focused research on specifically dark patterns is still emerging. Notably, the FTC held a workshop dedicated to dark patterns April 29 2021 to start bringing this critical issue "to light" (*Bringing Dark Patterns to Light*, 2021).

Like dark patterns, the concept of privacy engineering is not necessarily new, but attention and focus has received predominant attention more recently. This is likely due in large part that while companies have had privacy policies in the past, it is with the increase and greater pressure of policy measures such as the GDPR that companies have had a regulatory incentive to place concerted emphasis on this role. To this end, many of the large tech companies such as Google, Apple, Facebook, Twitter, and others are hiring dedicated teams of privacy professionals with the moniker of privacy engineer. As one example of a response to such an increase in demand, Carnegie Mellon has developed a privacy engineering program.

In practice, the National Institute of Standards and Technology (NIST) provides an entire privacy framework and defines privacy engineering as, "Focuses on providing guidance that can be used to decrease privacy risks, and enable organizations to make purposeful decisions about resource allocation and effective implementation of controls in information systems" (National Institute of Standards and Technology, 2020). Further, while there many theoretical approaches to privacy, one of the most dominant is Ann Cavoukian's systems approach of Privacy by Design (Cavoukian, 2009). Originally theorized in the late 90s, this approach requires privacy to be taken in account during the whole engineering process. Cavoukian solidified this concept into seven foundational principles, which were later adopted by the International Assembly of Privacy Commissioners and Data Protection Authorities. The EU GDPR also adopts a Privacy by Design approach, which includes most notably the foundational principle of "data protection by design and by default." One of the major critiques of Privacy by Design approach is that without sufficient regulatory "teeth," the design principle remains a voluntary and vague approach for corporations (Rubinstein & Good, 2012).

Research questions

This paper examines the topic of platform governance and digital rights online via the lens of privacy controls. The study seeks to build on existing privacy literature by examining how a platform's choices in updating privacy controls address relevant concerns and shifts in privacy expectations. Further, this project examines the embedded assumptions and implications of technology and technical design on society. The research questions are:

1. How do changes to privacy controls reflect evolving expectations of privacy online? What privacy issues are platforms attempting to address in privacy control changes?
2. What are the social and legal and economic inflection points that have precipitated these changes?

Materials and Methods

While the phenomenon of deceptive interface is not new, dedicated research on dark patterns is still emerging. One current focus is on identifying dark patterns and establishing definitions (Bösch et al., 2016; Gray et al., 2018). This paper is particularly interested in two types of dark patterns: 1. Privacy Zuckering ("deliberately confusing jargon and user-interfaces"), 2. Bad Defaults (pre-set options that cause users to unknowingly share more information than they may have wanted) (Bösch et al., 2016). Further, this paper applies Mathur et al.'s (2021) theoretical framework, which offers four possible lens to consider dark patterns: individual welfare, collective welfare, regulatory objectives, and individual autonomy. To this end, this study considers the major changes to privacy controls in relation to the normative values identified by Mathur et. al to examine how these changes reflect (or not) shifts in privacy expectations.

This paper addresses the role and power of technology companies in developing privacy policies, practices, and choices for their users. The privacy decisions of platforms affect billions of users worldwide. This study focuses on Facebook's history of changes to privacy controls as they remain one of the largest, most powerful, and oldest of the social media platforms. Facebook policies and practices have also borne great scrutiny—especially in recent years since the Cambridge Analytica revelations—from societal, legal, economic, and regulatory perspectives.

There are multiple locations where social media platforms present and implement their privacy and security policies including internet infrastructure, terms of service, privacy policies, public releases and statements, and privacy controls. The dataset for this paper is constituted of all Facebook Newsroom releases addressing privacy information, announcements, and updates. The Facebook Newsroom covers the public-facing press releases and news items from all aspects of Facebook: Facebook app, Messenger, Instagram, WhatsApp, Workplace, Oculus, Portal, and Novi. The news releases are presented chronologically, with most recent news items appearing first. It is possible to search the Newsroom through keyword searches or by topic. The topics are: Company News, Data and Privacy, Technology and Innovation, Safety and Expression, Election Integrity, Combating Misinformation, Economic Opportunity, and Strengthening Communities. Each news release is tagged with one or more of these topics.

The dataset for this study included all Facebook Newsroom releases discussing privacy. In order ensure collection of all articles relating to privacy, two searches were run on the Newsroom. Both searches focused only on Facebook, Facebook App, and Messenger news items (WhatsApp, Instagram, Workplace, Oculus, Portal, and Novi were cleaned from the data collection). First, a search was conducted of all Facebook's designated "Data and Privacy" articles. And the second search included a keyword search for "privacy" on the Newsroom articles. The results of this second search were cleaned for duplicates and non-privacy related news items. The time frame of this data collection included all Facebook Newsroom articles from the start of the Newsroom until the point of data collection in May 2021. The total dataset included 115 articles.

We note that the Facebook Newsroom is run by Facebook and presents a distinctly Facebook-centric perspective on news items. As full historical data on deployment of privacy controls is not readily or publicly available, the Newsroom serves as an effective dataset as the releases address not only the changes/updates made to settings, but often also acknowledge Facebook's reasoning and rationale for these changes, and as such, provide further insight into the socio-cultural and regulatory context.

Findings

This study considers Facebook's privacy control changes through a dark patterns theoretical framework (Brignull, 2010; Luguri & Strahilevitz, 2021; Mathur et al., 2021). Dark patterns are part of the underlying online design architecture, complicating communication processes, the flow of information, and affecting user control of data, privacy, and security. Dark patterns are everywhere and impact all aspects of our life online and need to be considered in internet policy and regulation.

The dataset of this study included 115 Facebook Newsroom articles on the topic of privacy, collected from the start of the Newsroom in 2006 to the time of data collection in May 2021. Of these 115 total articles, 76 articles addressed privacy controls. Figure 1 visualizes the overall breakdown of privacy articles by year, with the line indicating the corresponding number of articles addressing privacy controls. That two-thirds of Facebook Newsroom articles on the topic of privacy specifically mention privacy controls, emphasizes the normative, practical, and social value of privacy controls for Facebook.

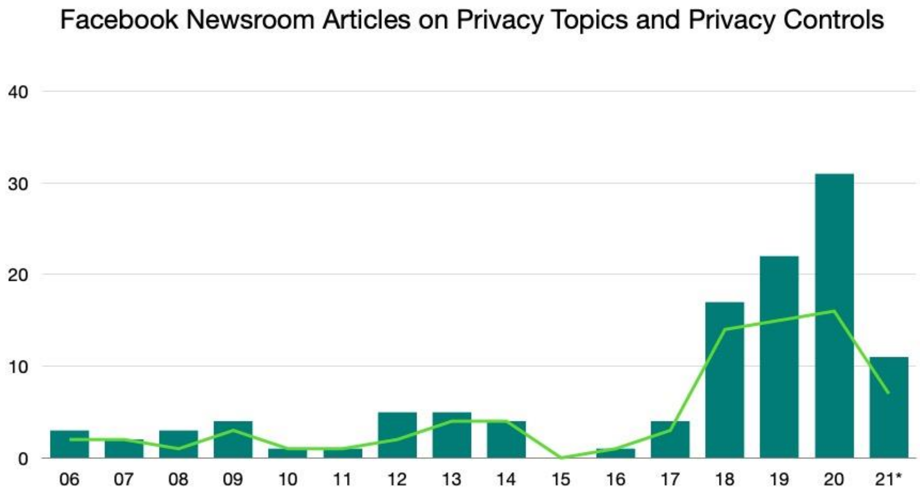

Figure 1

In 15 years, Facebook has changed or updated their privacy controls over 30 times. Some of these changes include large-scale privacy center makeovers, while some updates include only a handful of new controls, and other changes have included smaller or singular fixes. For example, one of the first major overhauls of the privacy controls was in 2010 when Facebook made efforts to simplify the settings pages. According to Facebook, they "reduced the number of settings required to make all information private from nearly 50 to less than 15," "consolidated 10 settings on 3 separate pages into 7 settings on one page," and "introduced presets that cover 18 individual settings for sharing with one single control—two clicks to control what had been more than 100 different options" ("Facebook Redesigns Privacy," 2010). However, even though Facebook efforts were in response to "the number one thing we've heard is that many users want a simpler way to control their information," the privacy controls were met with criticism. The Electronic Frontier Foundation (EFF) remarked upon the difficult to navigate privacy controls and pages, dubbing the roll-out an "Evil Interface" (Jones, 2010). The EFF has and continues to track and document the changes to Facebook's privacy controls and the challenges they may present to users and user privacy.

Notably, when highlighting changes to privacy controls, Facebook articles repeatedly and historically deploy the rhetoric of "choice and control" to indicate that users have agency and autonomy in deciding their privacy options. This rhetoric is significant in that it maps directly to Mathur et. al's (2021) normative lens of individual autonomy: "Autonomy is the normative value that users have the right to act on their own reasons when making decisions." In other words, when faced with regulatory action, legal penalty, or societal pressures, Facebook points to user controls as both a tool to address systemic privacy problems as well as a salve to their responsibility in privacy issues. As Facebook reminds users, people have "complete control" over their privacy choices.

For the purposes of discussing the findings on the significance of the role of privacy controls in the context of regulatory objectives, a closer look at two FTC settlements with Facebook offer insight into Facebook's allegedly deceptive privacy practices, policies, and settings. Returning to the dataset, the sudden increase of Newsroom articles on privacy in 2018 and subsequent years, tracks with the Cambridge Analytica revelations as well as the implementation of the GDPR. The previous small surge in articles in 2012-2014, indicate a company response to the original 2012 FTC settlement with Facebook. In this first settlement, Facebook had to give "clear and prominent notice and obtaining their express consent before sharing their information beyond their privacy settings, by maintaining a comprehensive privacy program to protect consumers' information, and by obtaining biennial privacy audits from an independent third party" (*FTC Approves Final Settlement With Facebook*, 2012).

In response to the August 2012 settlement, Facebook Newsroom released one article in November 2012 announcing proposed changes to privacy and policies, followed by two articles in December 2012. The first indicated the results of a global vote on the proposed changes and the second announced three major updates of "better controls to better manage your content" (Lessin, 2012). These updates included the introduction of privacy shortcuts to find controls more easily, improved "in-product education" to increase understanding, and new tools to remove oneself from tags. The next two years also see several updates to Facebook privacy practices. Notably, an update in 2013 switched the default sharing option from public to friends for teen users, which was soon followed by a general change of all users' default sharing from public to friends in 2014. This update addressed concerns about overly permissive default settings—also called "bad defaults"—and ties into both the dark patterns normative lenses of individual welfare and collective welfare.

Later in 2018, Facebook announced that it suspended Cambridge Analytica and the Strategic Communication Laboratories (SCL) Group from their site. As part of the release, Facebook acknowledged that 270,000 users downloaded Dr. Aleksandr Kogan's "thisisyourdigitallife" app and in doing so the users "gave their consent to access information such as the city they set on their profile, or content they had liked, as well as more limited information about friends who had their privacy settings set to allow it." In short, the app was able to download Facebook data from app users, and also from the Facebook friends of those users, leading to the access of millions of users' data. As Senator Ron Wyden (2018) noted, "Though Facebook offered an obscure privacy setting to disable that type of access, the setting was not advertised, nor was it disabled by default."

The final 2019 FTC settlement, which fined Facebook for a record $5 billion to settle FTC charges that Facebook violated the 2012 order, focused on privacy concerns. One of the FTC complaints included that despite the new tools Facebook rolled-out after the 2012 order, "These services, however, allegedly failed to disclose that even when users chose the most restrictive sharing settings, Facebook could still share user information with the apps of the user's Facebook friends—unless they also went to the "Apps Settings Page" and opted out of such sharing" (*FTC Imposes $5 Billion Penalty*, 2019). Amongst other complaints, the FTC also, "alleges that Facebook misrepresented users' ability to control the use of facial recognition technology" as the setting for facial recognition was called "tag suggestions" and enabled by default (*FTC Imposes $5 Billion Penalty*, 2019). The regulatory objectives of this FTC settlement target specifically difficult to navigate privacy settings ("Privacy Zuckering") and "bad defaults" that set users settings as overly permissive by default. In this case, the individual welfare and collective welfare of users as well as individual autonomy was impacted by these privacy controls, as well as users' individual autonomy.

Conclusion

This paper offers an examination of how Facebook engages with privacy through changes and updates to privacy controls over the years. In particular, the evolution, deployment, and use of privacy controls may offer key insight into privacy in action. As scholars have demonstrated the privatization of internet governance through privacy policies, infrastructure, architecture, and content moderation policies, this paper suggests that privacy controls should also be considered within this framework.

Dark patterns can impact democracy and user agency, with harms ranging from privacy and financial harms to freedom of choice. This study contributes to an emerging topic in internet governance and builds upon the growing literature on dark patterns, which address deceptive practices and their impact on privacy online. Ongoing policy debates are now considering dark patterns and if and how they can be regulated. Understanding the role of privacy controls in the context of privacy rights and data rights of users and how companies such as Facebook update their settings in response to critical inflection points, may have profound impact in the governance, policy, and regulation of platforms.

Works Cited

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

Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies*, *2016*(4), 237–254. https://doi.org/10.1515/popets-2016-0038

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

Brignull, H. (n.d.). *Dark Patterns*. Retrieved April 24, 2021, from https://www.darkpatterns.org/

Bringing Dark Patterns to Light: An FTC Workshop. (2021, February 1). Federal Trade Commission. https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop

Calo, R. (2013). *Digital Market Manipulation* (SSRN Scholarly Paper ID 2309703). Social Science Research Network. https://doi.org/10.2139/ssrn.2309703

Carmi, E. (2020). *Media Distortions*. Peter Lang.

Carmi, E. (2021, April 7). *Nick Clegg and Silicon Valley's myth of the empowered user—Elinor Carmi*. Tech Policy Press. https://techpolicy.press/nick-clegg-and-silicon-valleys-myth-of-the-empowered-user/

Cavoukian, A. (2009). The 7 Foundational Principles. *Information and Privacy Commissioner of Ontario*, 2.

Chun, W. H. K. (2006). *Control and freedom: Power and paranoia in the age of fiber optics*. MIT Press.

Clegg, N. (2021, March 31). *You and the Algorithm: It Takes Two to Tango*. Medium. https://nickclegg.medium.com/you-and-the-algorithm-it-takes-two-to-tango-7722b19aa1c2

Criado-Perez, C. (2019). *Invisible women: Data bias in a world designed for men*. Abrams Press.

DeNardis, L., & Hackl, A. M. (2015). Internet governance by social media platforms. *Telecommunications Policy*, *39*(9), 761–770. https://doi.org/10.1016/j.telpol.2015.04.003

Dencik, L., & Cable, J. (2017). Digital Citizenship and Surveillance| The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks. *International Journal of Communication*, *11*(0), 19.

Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., & Bacchelli, A. (2020). UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–14. https://doi.org/10.1145/3313831.3376600

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

Facebook Redesigns Privacy. (2010, May 27). *Meta*. https://about.fb.com/news/2010/05/facebook-redesigns-privacy/

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

Fried, I., & Allen, M. (2021, March 21). *Exclusive: Trust in tech cratered all over the world last year*. Axios. https://www.axios.com/edelman-trust-barometer-tech-5787acea-8ef5-4d0b-9694-6e4f8eb006c4.html

FTC Approves Final Settlement With Facebook. (2012, August 10). Federal Trade Commission. https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook

FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. (2019, July 24). Federal Trade Commission. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

Gillespie, T. (2010). The politics of 'platforms.' *New Media & Society*, *12*(3), 347–364. https://doi.org/10.1177/1461444809342738

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–14. https://doi.org/10.1145/3173574.3174108

Jones, T. (2010, April 29). *Facebook's "Evil Interfaces."* Electronic Frontier Foundation. https://www.eff.org/deeplinks/2010/04/facebooks-evil-interfaces

Lessin, S. (2012, December 21). Better Controls for Managing Your Content. *Meta*. https://about.fb.com/news/2012/12/better-controls-for-managing-your-content/

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

MacKinnon, R. (2013). *Consent of the networked: The worldwide struggle for Internet freedom* (Paperback edition). Basic Books.

Mathur, A., Mayer, J., & Kshirsagar, M. (2021). What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–18. https://doi.org/10.1145/3411764.3445610

National Institute of Standards and Technology. (2020). *NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0* (NIST CSWP 01162020; p. NIST CSWP 01162020). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.01162020

National Intelligence Council. (2021). *Global Trends: A More Contested World*. https://www.dni.gov/index.php/global-trends-home

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

Rubinstein, I., & Good, N. (2012). *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents* (SSRN Scholarly Paper ID 2128146). Social Science Research Network. https://doi.org/10.2139/ssrn.2128146

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

Sunstein, C. R. (2013). Deciding by Default. *University of Pennsylvania Law Review*, *162*(1), 1–58.

Sunstein, C. R. (2019). SLUDGE AND ORDEALS. *Duke Law Journal*, *68*(8), 1843-.

Svirsky, D. (2019). Why do people avoid information about privacy? *Journal of Law & Innovation*, *2*(1).

Vaidhyanathan, S. (2018). *Antisocial media: How facebook disconnects US and undermines democracy*. Oxford University Press.

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

Zuboff, S. (2020). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (First Trade Paperback Edition). PublicAffairs.

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