

Deceptive Digital Design in Google Applications

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Cecilia Smith

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Benjamin J. Laugelli, Assistant Professor, Department of Engineering and Society

Introduction

Google is one of the most well-known global technology companies of the digital age. With their large user base, they have a broad reach to many diverse types of users and, subsequently, numerous platforms from which to collect data. Since Harry Brignull coined the term “deceptive designs” in 2010, users and user experience (UX) experts have become critically aware of “tricks used in websites and apps that make you do things that you didn't mean to” (*Deceptive Design*, n.d.). For Google, this primarily appears as deceiving features (or lack of any features) to mislead users into sharing more personal tracking information than they intend to or are aware of. This includes location data, search history, and web activity. For this research, I will be investigating Google’s general account settings page as well as its Google Maps and Gmail services. It is important to note that while most users are aware they are sharing *some* personal information by the nature of their digital activity, they are not fully informed regarding the quantity or alternative options to reduce collection of their personal data.

In recent years, Google has received several lawsuits regarding its privacy practices. In fact, “between September 2022 and January 2023, Google has settled a series of sweeping privacy lawsuits, resulting in nearly \$600 million in historic settlement payouts to states and affected users” (Demers, 2023). Most recently, according to a complaint filed in January 2023, “Google intentionally exploited its massive trove of user data to further entrench its monopoly across the digital advertising industry” (Department of Justice, 2020, p. 13-14). While these lawsuits are for a myriad of privacy issues, spanning from advertising to location data, the trend demonstrates that once users (both individuals and organizations) learn about the quantity of their data being collected by Google and its applications, such as Google Maps, along with how the data is used, they are unsatisfied with the manner in which they were previously informed

about these practices. However, this understanding fails to consider the methods Google uses to collect this data and the ethical implication of its UX design choices. It is critical to understand how Google's UX design choices and intentional inclusion of deceptive practices mislead users. If we do not consider how users are deceived, then we will not recognize how Google is violating principles of care ethics. With this understanding, users will be better informed and will have the agency to proactively protect their privacy. Basing this analysis on the conceptual framework of care ethics allows us to examine the moral decisions made in favor of or against other actors. Care ethics is an ethical framework that focuses on care as a virtue, specifically considering how relationships are affected by an individual's decisions. Using a 2016 report, *The Economics of Privacy*, published in the Journal of Economic Literature and a study conducted by researchers from Purdue University (2018) along with primary examples from various Google interfaces, I will demonstrate how Google's practice of deceptive designs violates care ethics by taking advantage of its power over users and neglecting transparency throughout its account settings.

Background

In 2010, Harry Brignull coined the term "deceptive designs" (also known as, "dark patterns") and created a website educating users and UX designers on the twelve main types of deceptive practices in UX design (*Deceptive Design*, n.d.). This website also serves as a platform to call out deceptive practices when users spot them anywhere online. The main companies with callouts are Google, Facebook, Amazon, LinkedIn, Microsoft, and Apple. I will be exploring instances of privacy zuckering and confirmshaming, which are types of deceptive designs, within Google Maps, Gmail, and general Google account settings, as explained further in the Analysis

section. With growing awareness of deceptive design practices, some UX designers have thoughtfully analyzed user values to propose alternatives to existing practices. As Kollnig and others proposed at the 2021 CHI Conference on Human Factors in Computing Systems (2021), it is possible to embed customization options for users, so they could curate their interfaces according to the way they prefer content to be presented (Kollnig et al., 2021, p. 2). Similarly, Parrilli and Hernández-Ramírez (2020) promote switching the traditional order of default privacy settings such that interfaces highlight the most conservative and restrictive privacy settings instead of hiding these options deep within an interface's settings (Parrilli & Hernández-Ramírez, 2020, p. 253). This is an example of the potential evolution of the UX industry, as users, designers, and platform operators take action to combat deceptive practices similar to those outlined in the following research.

Literature Review

Currently, scholars have determined the negative ethical implications of deceptive design patterns. They have also addressed users' concerns for digital privacy, especially as more daily activity is conducted online. However, scholars fail to address how these deceptive designs are exploiting user data at the request of digital companies, specifically Google. Users have become increasingly aware of how their data is collected and used by digital companies, and upon investigation, most platforms are collecting more data than users are aware. Furthermore, "while research shows that many of the people who are involved in online activities are aware that their personal data is being collected and shared, this gives no concrete proof to assume that people are willing to give away their personal data" (Human & Cech, 2020, p. 141). This caveat of user awareness regarding their personal data is an important consideration highlighted by the

concerns of the scholars below regarding digital designs and digital privacy. Both Acquisti and others with the *Journal of Economic Literature* (2016) and Gray and others from Purdue University (2018) research these concerns but fail to apply care ethics to the current digital data environment and, more specifically, to Google.

In 2016, Alessandro Acquisti, Curtis Taylor, and Liad Wagman researched the current sentiments of Internet users in the context of an increasing economic motivation for companies to collect user data. According to a 2015 study conducted by the Pew Research Center, “an overwhelming majority of US adults (93 percent) believe that being in control of who can get information about them is important; but only 9 percent of them think that they have, in fact, ‘a lot’ of control over how much information is collected about them and how it is used” (Acquisti et al., 2016, p. 476). The researchers argue that these findings warrant discussion of the “privacy paradox” where digital users value privacy; however, they are willing to compromise some of their personal information in order to use digital resources to their full potential (Acquisti et al., 2016, p. 476). Asymmetric information (when one party has more information than another) has contributed to this paradox as “some individuals may not be aware of the extent to which their personal information is collected and identified online... or, some individuals may not be aware of possible alternative solutions to their privacy concerns” (Acquisti et al., 2016, p. 477). These scholars have identified that data privacy is a major concern for digital users; however, users are not sufficiently informed of their privacy risks and agreements when using different platforms. Current literature fails to consider the role of care ethics in digital companies’ decision making and how this affects users with less decision-making power. I will build upon the existing research by using Google as a case study to demonstrate how intentionally deceptive designs are challenging users’ desire for control over their personal information.

In 2018, a group of researchers, led by Colin M. Gray, from Purdue University identified ethical concerns associated with deceptive design practices and provided additional context for why users feel they are lacking control over their personal data, just as Acquisti and others concluded. These researchers identify the natural tendency for digital platforms to guide users to complete certain actions or view specific content by “[acknowledging] the persuasive intent underlying all of design activity” (Gray et al., 2018, p. 3). They argue that deceptive designs have veered from this natural tendency and instead towards a manipulative and immoral practice at the expense of users and their privacy. Gray and others acknowledge that there exist ethical concerns with deceptive design practices, especially once the motivations of digital platforms and their UX designers are considered; however, they do not consider care ethics as a measure of ethical practices.

Both groups of researchers led by Acquisti (2016) and Gray (2018) have identified major privacy concerns for digital users along with minimal explanatory material regarding data collection practices on digital platforms. Existing scholarly literature acknowledges the unequal power distribution between digital companies and their users, particularly as platforms are inherently designed to guide users to complete certain tasks. However, scholars have not yet adequately considered the extent to which Google has contributed to user distrust and misunderstanding surrounding their digital privacy. Due to Google’s expansive global reach, with an estimated user population of over one billion, its data collection practices should be examined closely (Djuraskovic, 2022). By investigating the ways in which these parties interact through digital interfaces, my research will fill a gap in the understanding of the role of care ethics across Google platforms.

Conceptual Framework

Care ethics is a derivation of virtue ethics, where care as a virtue centralizes relationships as a driving force of personal interactions and technological decisions. Care ethics “emphasizes the importance of relationships” and identifies how moral obligations can influence the decisions made when connecting across different relationships (van de Poel & Royakkers, 2011, p. 102). To uphold care ethics, attentiveness, responsibility, competency, and responsiveness must be maintained when interacting with external stakeholders (van de Poel & Royakkers, 2011, p. 102). Attentiveness, also known as “caring about,” requires individuals to perceive others’ needs and prioritize which needs should receive additional care and consideration (Tronto, 1998, p. 16). Responsibility, or “taking care of,” is obtained when one individual or group commits to caring for another. Competency is considered the “caregiving” phase once someone’s needs have been identified and taken responsibility for and then these needs can be met and cared for. This phase often requires the most ethical consideration because there must be full awareness of all stakeholders’ needs and concerns. Finally, responsiveness involves analyzing a situation to determine if proper care has been administered and how care can be adjusted to better serve those providing and receiving care (Tronto, 1998, p. 17). Together, these four stages of care ethics depict the entire process of caring “well;” however, it is important to note that power dynamics among relationships can make each of these phases difficult to uphold. These values will define the social responsibility of all actors in practice and will be used to analyze the relationships between those in control of UX design and those consuming the content.

For this analysis, it is critical to acknowledge the power dynamics among relationships, especially the moral responsibility to protect those in vulnerable positions. In the context of care ethics, asymmetric power distributions enable one party to have more power in decision making

and implementation over another group. This can also affect indirect stakeholders who will be impacted by decisions in which they have no decision-making power. This is illustrated among the UX industry in general where sector experts have identified the unique disparity existing around UX designs and have articulated that “the most vulnerable to these [deceptive design] patterns are those consumers with less education, lower-income, and those experiencing negative life events... And, of course, those furthest from the creation of the manipulative design” (Riggins, 2022). While users and their personal matters are distant from UX designers, those with the power to create digital platforms are accountable to maintain values of “good care.” Failure to consider these factors can result in an asymmetric power relationship, which can make it difficult to properly uphold the four phases of care ethics. The following sections will explore two different examples of deceptive design and the practices of care ethics associated with these decisions.

Analysis

Google misleads users into sharing more personal data than they are aware of by using two deceptive UX designs, which violates principles of responsible care ethics. I will demonstrate these practices and explain the two forms of deceptive design that are violated. Privacy zuckering and confirmshaming will be articulated within their role on Google’s platforms. This analysis will demonstrate Google’s violation of *attentiveness* and *responsibility* to its users and their digital privacy within the context of care ethics.

Privacy zuckering

Google fails to act with responsible care ethics by implementing privacy zuckering across its platforms. Here, I will illustrate this violation of user location data, within the Google Maps application and within general Google account usage. Named by Tim Jones and shared by Harry Brignull, “privacy zuckering” refers to the practice of misleading users to share more personal information, both publicly and with platform operators, than they intend to” (*Privacy zuckering - A type of deceptive design*, n.d.) This term makes reference to Mark Zuckerberg, CEO of Facebook, because Facebook has notoriously collected user information without full transparency; however, the focus here will remain on Google. The critical component of privacy zuckering consists of features or materials within a platform that ignore or cover up key details regarding user privacy settings. A common example includes lengthy Terms and Conditions statements containing information about which types of user data will be collected, such as location data, personal contacts, and financial information.

Google turns location tracking on for users by default. Even if users were to find this detail in the Terms and Conditions upon creating their account, there is no option to opt out of this tracking until their account is created. As discussed in the following section, deleting this data once it has been collected is a cumbersome process. Privacy zuckering neglects to uphold attentive and responsible care, particularly as the UX designers have greater power in setting the defaults for a user account. As seen below, *Figure 1: Google Maps location settings* is a screenshot of user settings within the Google Maps mobile application, where both Location History and Web & App Activity are being collected by default. Users would not know this information unless they went into their settings and perused through the pages.

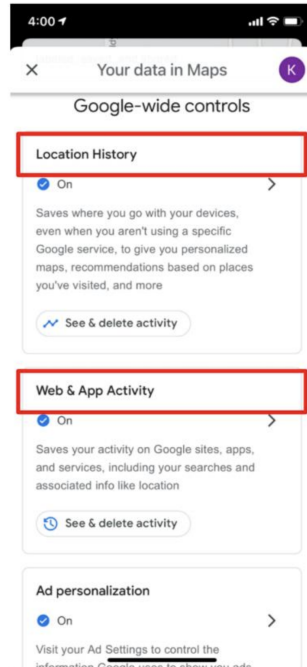


Figure 1: Google Maps location settings (McNealy & Nguyen, 2021, p. 22)

As Fisher and Tronto (2019) articulate, “caring about [attentiveness] involves paying attention to our world in such a way that we focus on continuity, maintenance, and repair. Taking care of [responsibility] involves responding to these aspects-taking responsibility for activities that keep our world going” (Fisher & Tronto, 1990, p. 40). In this case, Google is not taking responsibility for the activities of data collection and data privacy. It is taking advantage of users’ lacking technical knowledge instead of protecting their personal information. Privacy zuckering design components target these principles of care ethics when they are lacking because users are vulnerable to what they do not know.

Without clear communication of default privacy settings, UX designers are neglecting their corporate social responsibility, which is a direct violation of care ethics (van de Poel & Royakkers, 2011, p. 103). This responsibility includes stakeholders considering how they, “as part of the enterprise[,] can best deal with the interests and rights of others” (van de Poel & Royakkers, 2011, p. 103). For Google, this would include acting in support of its users’

preferences to protect their privacy. Richard Devon's proposed "norms of engagement" for engineers include "democratic information flow," which is expected to be understood and upheld across groups of engineers and non-engineers (van de Poel & Royackers, 2011, p. 104). As UX designers are not freely sharing information about users' data privacy, these norms of engagement within care ethics are not met. Therefore, Google and its UX designers are not acting responsibly with regards to care ethics.

As I have argued above, Google is violating care ethics by restricting information shared with its users regarding their data collection. Some argue that the data collected serves a positive purpose by improving user experience with personalized advertisements and search-results content. However, this view fails to consider the interests of users and the methods companies use to acquire user data while they are using digital platforms. Purdue University's Shruthi Sai Chivukula, Jason Brier, and Colin M. Gray performed a study (2018) and found that although designers recognize user values, they often prioritize client values in final designs (Chivukula et al., 2018, p. 90). Some of the user values they recognized were the following: "right to information, usability, security, flexibility, automation, optimization, trust, and aesthetics" (Chivukula et al., 2018, p. 90). When designers were working to persuade users to achieve client goals, they implemented deceptive designs. While some users are comfortable with sharing their private data, deceptive designs take away the agency to make this choice leaving users unaware they have agreed to share their data in the first place. With regards to transparency, Google is withholding the details of its data collection to users and, therefore, assuming that users prefer to have tracking settings turned on by default. These practices violate user privacy and do not uphold principles of responsible care ethics.

Confirmshaming

Google's lengthy and complex process to delete user location data ends with "confirmshaming" and challenges users to complete their intended action and neglecting their interests, which is a violation of care ethics. Confirmshaming, coined by Harry Brignull, occurs when UX features are designed to inflict guilt or regret and persuade users to stop proceeding with their current task. Below, *Figure 2: Gmail example of confirmshaming* illustrates a common scenario for this strategy, where the user is trying to opt out of a service, but the platform is presenting bias to convince the users that doing so is a poor judgment (*Confirmshaming - A type of deceptive design*, n.d.). The wording "I don't want smarter email" implies that opting out of Gmail on this user's mobile device would have negative functional consequences.

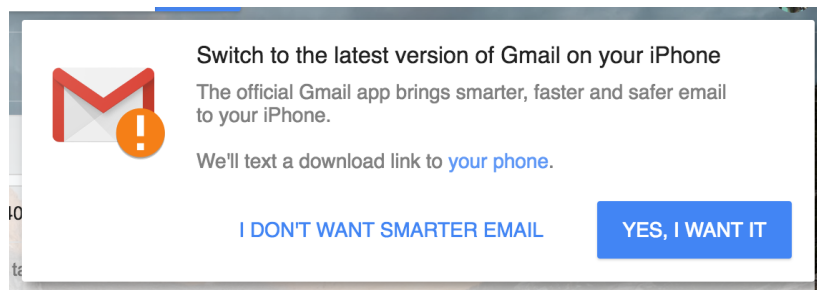


Figure 2: Gmail example of confirmshaming (Confirmshaming - A type of deceptive design, n.d.)

This Gmail pop-up provides a glimpse into confirmshaming techniques. In this instance, the user's choices will affect how they access Gmail (i.e. mobile application or a desktop application); however, Google's use of confirmshaming features regarding user location data impacts how much information is collected from users. Below, *Figure 3: Google example of confirmshaming* is a screenshot of a personal Google account attempting to pause their location history.

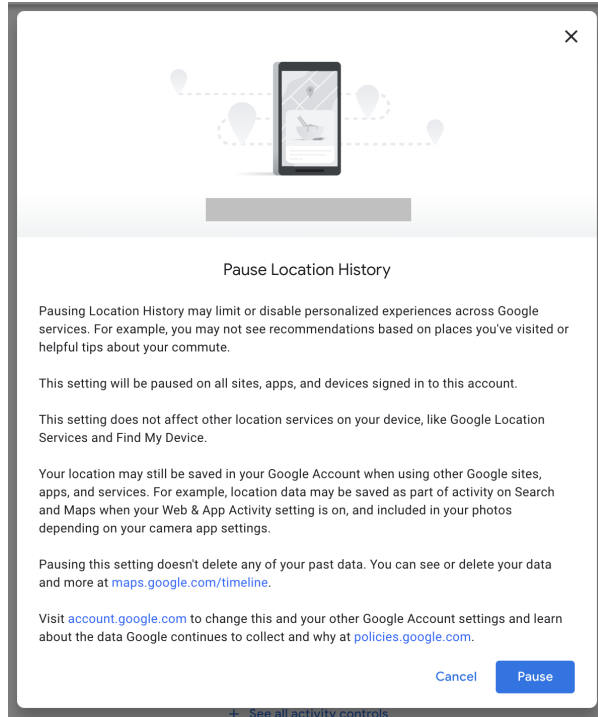


Figure 3: Google example of confirmshaming

As seen in the first paragraph of the pop-up, the text implies that pausing this data collection will decrease the quality of Google services. Additionally, the fifth paragraph provides a link to view and manage other location data. However, upon moving to this page, deleting the data in its entirety is not straightforward. Implementing deceptive design to shame users into opting out or removing services restricts their ability to make informed decisions.

Confirmshaming provides another example of a violation of care ethics when one party, the UX designers, has greater power than the users. In this case, the power lies in knowledge and awareness of technological fields and data privacy practices. Fisher and Tronto (1990) explain the way in which groups in power, such as UX designers and Google, should act in order to protect the best interests of those impacted by their technology with the following: “[A] group engages in taking care of a person or thing or situation, we expect them to find the resources required to fulfill that responsibility. Thus, the notion of *taking care of* has built into it assumptions about power, that is, about the ability not only to predict and to judge but to

command resources” (Fisher & Tronto, 1990, p. 43). Therefore, *taking care of* includes predicting and judging what knowledge and resources impacted groups will need to properly and responsibly use a technology. Unfortunately, by shaming users from opting out of location tracking, Google is doing the opposite of providing opportunities for fair knowledge sharing. Google and its UX designers provide only vague descriptions about the consequences of pausing tracking, and stating that this decision “may limit or disable personalized experiences across Google services” leaves users doubtful about their initial goal, see *Figure 2: Google example of confirmshaming*. According to previous experience and cultural norms, users among the general public will most likely value the viewpoints and suggestions of engineers and technology companies higher than their own knowledge. Google is abusing this position of power to mislead users with vague, yet pessimistic outlooks regarding the consequences of pausing location tracking. In doing so, Google is ignoring their responsibility to take care of their users and their interests in personal privacy. As such, this is a violation of the principles of care ethics.

Conclusion

In its efforts to collect user data, Google has implemented deceptive design practices, such as privacy zuckering and confirmshaming, and has neglected to consider user interests. These deceptive designs are created to mislead users about how their data is collected and used and, therefore, violate responsible care ethics practices. Google is failing to uphold both the attentiveness and the responsibility phases of care ethics with regard to its users and their personal digital privacy. The consequences of these design choices are decreased agency for users to make decisions regarding their own privacy and tainted trust for users, as they are not

presented with clear, concise descriptions of how their data is collected and how it can be managed.

References

- Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature*, 54(2), 442–492. <https://doi.org/10.1257/jel.54.2.442>
- Chivukula, S. S., Brier, J., & Gray, C. M. (2018). Dark intentions or persuasion? UX designers' activation of stakeholder and user values. Dis 2018: Companion Publication of the 2018 Designing Interactive Systems Conference, 87–91. <https://doi.org/10.1145/3197391.3205417>
- Confirmshaming—A type of deceptive design.* (n.d.). <https://www.deceptive.design/types/confirmshaming>
- Deceptive Design.* (n.d.). Deceptive Design. <https://www.deceptive.design/about-us>
- Demers, B. (2023, January 12). Google racks Up \$600M in privacy settlements across U.S. How much will users get? Kiplinger. <https://www.kiplinger.com/personal-finance/google-privacy-settlements>
- Department of Justice. (2020, October 20). Justice Department Sues Monopolist Google For Violating Antitrust Laws—Complaint. The United States Department of Justice. <https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws>
- Djuraskovic, O. (2022, December 26). Google search statistics and facts 2023 (you must know). First Site Guide. <https://firstsiteguide.com/google-search-stats/>
- Fisher, B., & Tronto, J. (1990). Toward a Feminist Theory of Caring. *Circles of Care*, 35–62. State University of New York.
- 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 (CHI 2018). <https://doi.org/10.1145/3173574.3174108>

Human, S., & Cech, F. (2020). A Human-Centric Perspective on Digital Consenting: The Case of GAFAM. In A. Zimmermann, R. J. Howlett, & L. C. Jain (Eds.), *Human Centred Intelligent Systems*, 189, 139–159. Springer, Singapore.

https://doi.org/10.1007/978-981-15-5784-2_12

Kollnig, K., Datta, S., & Van Kleek, M. (2021). I Want My App That Way: Reclaiming Sovereignty Over Personal Devices. *Extended abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–8. <https://doi.org/10.1145/3411763.3451632>

McNealy, J., & Nguyen, S. (2021). *I, Obscura*. Stanford Digital Civil Society Lab (DCSL). https://issuu.com/stanforddcsll/docs/dcsll_darkpatternsziine_2021

Parrilli, D. M., & Hernández-Ramírez, R. (2020). Re-Designing Dark Patterns to Improve Privacy. *2020 IEEE International Symposium on Technology and Society (ISTAS)*, 253–254. <https://doi.org/10.1109/ISTAS50296.2020.9462197>

Privacy zuckering—A type of deceptive design. (n.d.).

<https://www.deceptive.design/types/privacy-zuckering>

Riggins, J. (2022, May 11). Critics of ‘Deceptive Design’ Push for a More Ethical UX. *The New Stack*. <https://thenewstack.io/critics-of-deceptive-design-push-for-a-more-ethical-ux/>

Tronto, J. C. (1998). An Ethic of Care. *Generations: Journal of the American Society on Aging*, 22(3), 15–20.

van de Poel, I., & Royakkers, L. (2011). *Ethics, Technology, and Engineering*. John Wiley and Sons.