Analyzing Deceptive Design in Cookie Consent Banners Through an Ethical Lens

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

Mary Victoria C. Streetman

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

MC Forelle, Department of Engineering and Society

Introduction

In 2018, the Facebook-Cambridge Analytical scandal revealed a dark side to our modern-day digital age, where personal data is no longer just a commodity, but a weapon in the hands of those with the power to manipulate and control. It was revealed that the political consulting firm Cambridge Analytica had harvested the personal data of millions of Facebook users without their consent, using it to create targeted political ads during the 2016 U.S. presidential election. Thanks to whistle blower, Christopher Wylie, and the public outcry following his tell-all interview, Facebook and Cambridge Analytica were held financially and legally responsible for their unethical behavior and lack of data privacy policies (Lewis, Pegg, & Hern, 2018). However, perhaps more significantly, this controversy sparked a global conversation about online privacy and data protection, raising crucial questions about the role and responsibilities of tech companies in safeguarding user information.

Many internet users believe that the conservation of privacy is at the inclination of "Big Tech", powerful technology companies like Facebook, and determined by the standards these corporations set for collecting, analyzing, and dispersing personal information. Therefore, many people view forfeiting their data as a necessary evil to function effectively in a modern world where the internet has become a critical tool for accessing important information, communicating with others, and conducting business.

For instance, when interacting with any kind of website, app, or browser, users are simultaneously having their data collected via cookies. Cookies are small text files sent by web servers and stored on web browsers that save user preferences and internet activity that can later be accessed by the browser and requesting applications. In general, cookies help make websites

easier to use or revisit by saving login information, account state, or setting preferences, and encourage users to spend more time on the application. However, businesses have monetized these features of ease and efficiency by selling user preferences to digital advertisers (Dembrow, 2022). Because advertisers significantly value this information, the lucrativeness of selling user preferences for targeted advertising or product development incentivizes companies to abuse this medium of user data collection.

Many applications utilize a graphical display called a “popup”, a window that appears on top of an application’s main interface, to alert the user of the use of cookies and or ask for the user’s consent to the usage of these cookies. However, there are often many flaws with the design of these consent forums. Specifically, there is evidence of cookie consent popups that utilize interface design elements that are “dark” or “deceptive”. The term, “dark pattern”, popularized by Harry Brignull (2013), refers to design elements that are intended to trick or persuade a user of an action that may not be in their best interest, but may be to the benefit of the business (Mejtoft et al., 2020; Maier & Harr, 2020). Deceitful design can take many forms in cookie consent popups, such as pre-checked boxes, misleading language, or confusing interfaces, and can result in users inadvertently providing consent to activities they do not fully agree with or understand (Mejtoft et al., 2020). Such design patterns can be seen as a violation of user autonomy because they prevent users from making informed decisions about their online activity and legitimately consenting to cookie use.

I contend that the inclusion of manipulative interface design elements in cookie popups gives rise to ethical concerns from the perspectives of both the utilitarian and rights theory, as the use of such dark design patterns poses a threat to user privacy, autonomy, and the integrity of consent acquisition, highlighting the need to adopt more transparent and user-focused design

practices in the tech industry. In addition, I explore the definitions of autonomy, privacy, and consent both outside and within the technology discipline to determine how these concepts apply to the design process and ethicality of technology. Ultimately, I describe the utilitarian and rights ethical theories and how they apply to cookies popups and dark design patterns. The findings of this research emphasize the importance of prioritizing user autonomy and privacy in the design process. In turn, encouraging current and future designers and web developers to analyze the ethicality and implications of their own projects and overcome the limitations of a traditional design process by rendering user interactions that emphasize inclusivity and morality. In doing so, lead the technologizing world to continually respect the rights and dignity of its users.

Literature Review

This literature review will explore the concepts of informed consent, autonomy, and privacy in relation to the ethical dilemma of deceptive elements of cookie consent popup forms. The review will also highlight the dynamics that exist between clients, tech companies, and the cookies that implement dark design tactics. While also summarizing the technicalities of the ethical frameworks utilized in the ethical analysis.

As previously discussed, cookies are used widely across nearly every kind of website and serve to collect data on users to improve functionality and user experience. However, there are tradeoffs and risks that are not always fully communicated or known by the users. The concern primarily stems from third-party cookies, cookies that are implemented on a user's browser by a domain different from the one the user is visiting. These third parties, including major data brokerages, online advertisers, and external tracking applications, gain access to the extensive user data utilized by visited web applications, which allows these organizations to create online activity profiles for specific users which are then sold or used for targeted advertising (Cahn et al., 2001;

Shah & Kesan, 2009). Even more terrifying, the abuse of these sophisticated analytics could lead to the denial or discrimination of service by the web application itself or numerous third-party companies based on a user's race or other defining characteristics determined by the collected data (Richards, 2014). Likewise, users are put at further social and economic risk due to the lack of security present. Some cookies are implemented in such a way that their data can be intercepted over network traffic by an "eavesdropper [who] can steal and reuse a cookie, impersonating a user indefinitely" (Sit, 2001, p. 120). By stealing a cookie, the hacker could gain access to valuable personal information such as login criteria for accounts that contain credit card or banking information (LaCroix, Loo, & Choi, 2017). The specific security and use of cookie data is largely unknown by the general internet consumer, and more significantly out of their control, limiting their ability to provide informed consent to cookie usage (LaCroix, Loo, & Choi, 2017). However, many web applications want to encourage users to allow cookies regardless of these risks because of financial incentives. Therefore, these web applications purposely utilize or ignore the use of deceptive design elements in their popups because they can help persuade users to consent to data collection via cookies.

To limit the scope of the ethical analysis, only the deceptive design elements obstruction and interface interference, two of the most prominent dark design elements in cookie popups, will be discussed. Obstruction is the utilization of design to make a process more complex or confusing, in an attempt to dissuade an action (Maier and Harr, 2020; Gray et al., 2018). For example, having to click through multiple links or windows to deselect cookies or deny their use. Interface interference is when elements of a user interface design are presented in a manner that one action will be favored over another (Maier and Harr, 2020; Gray et al., 2018). A simple case could be highlighting a particular button on the popup to catch a user's attention, encouraging them to click

that one over another. Or oppositely, making it difficult to see or read by using fine print to display links or relevant information regarding the cookie use of the application and the user's options.

However, simply having a consent interface that avoids manipulating users toward less privacy-protective options is not considered the standard for good consent acquisition. To be considered usable a consent interface should not only address users' needs but should also make it effortless for them to know and have equal access to all their options, understand what their choice implies, and be able to change their decision later (Cranor & Habib, 2023; Nielsen, 2020). In more concise terms, presenting users with an interface that encourages autonomy is the standard for consent acquisition. Autonomy refers to the ability of an individual to make decisions about their own life without interference from external forces. The medical field often focuses on upholding patient autonomy and can strongly serve as a model for how technology can preserve and heighten the wellbeing of users. The relationship between a doctor and patient is extremely imbalanced regarding knowledge of care, which might suggest the expert should be the sole decision maker regarding procedures on the patient's body. However, there are often many more elements that go into making these decisions beyond science and the medical solution, such as quality of life or religious beliefs. As a result, the medical field currently prioritizes and upholds their patients' decision-making ability and informed consent to mitigate any potential threat to their autonomy (Burton et al., 2019). Similarly, in the context of technology, there is often a large disparity of power and knowledge between the web designers and data analysts of an internet application and most users. Therefore, when cookie popups implement dark design patterns of obstruction and interface interference users are often incapable of providing informed consent. Informed consent refers to the process of obtaining permission from an individual before collecting or using their personal information and requires that individuals are knowledgeable about what

personal information is being collected, why it is being collected, how it will be used, and who it will be shared with (Burton et al., 2019). Based on the previous logic, the lack of informed consent puts a user's autonomy at risk.

Ultimately a cookie popup ought to collect informed consent. If consumers are not able to understand quickly and thoroughly who they are providing their data and what permissions they are granting regarding their data use, they will not be able to accurately access the risks of consenting to cookies. Therefore, the user will default to how much they trust a web application determined by the application's public reputation (Norberg, Horne, & Horne, 2007). This default response will lead to the decline of users' sense of personal privacy and control (Norberg, Horne, & Horne, 2007).

However, the idea of privacy has evolved drastically over time with societal changes and is defined differently by different people in a variety of contexts, making it quite hard to pinpoint its exact meaning (Bruton & Nissenbaum, 2015). For instance, in a personal context privacy provides anonymity and with it independent, free-thinking people. In business, privacy provides products, processes, and services value and individuality. In the newer technological context and the context of the outlined ethical dilemma related to cookie use, privacy protection and data protection are seen as synonymous since the issue is rooted in the unbridled methods of data collection and use. More concretely, the term privacy protection can be understood as, "the societal rules that govern collection, use and disclosure of personal data" (Minkkinen, 2019, p. 985). These norms are determined by public, and personal ethical conversations and based on the use of data and collection guidelines internet users are collectively willing to accept.

Cookie consent popup design elements that limit or prevent informed consent calls into question the ethicality of the utilization of these patterns by web designers and applications. The utilitarian ethical theory can be boiled down to the utility principle: that good and proper decisions are ones that create more positive consequences than bad, for the most amount of people (Velasquez et al., 2015; Schinzinger & Martin, 2000). This mindset can be organized into a balance sheet that compares the amount of expected welfare versus the pain produced by a given act. Each of the elements, on either side of the balance sheet, are valued based on the significance of their intensity, duration, certainty, proximity, and extent. Considering John Stuart Mill's concept of the freedom principle, the positive consequences of an action only deem the action as good if the action is not denying or hindering the pleasure of others (van de Poel & Royakkers, 2011). In the context of cookies, the act in question is the decision made by web designers to incorporate dark design patterns in cookie consent forms, intentionally or otherwise. Under utilitarianism the benefits and consequences of this decision are considered for significant actors including users that interact with these cookie popups, applications and web designers that implement them, advertisers and data analysts, and the government that all the previous fall under. And while the limitations of utilitarianism are such that it ignores the interpersonal relationships between actors, the unpredictability and uncertainty of the specific consequences of action before they occur, and the subjectivity of the measurement of well-being, this framework serves to provides a broader more societal perspective on the morality of deceptive design in digital consent acquisition (van de Poel & Royakkers, 2011).

To create a contrasting perspective, rights ethics emphasizes the inherent rights and dignity of individuals. In fact, rights ethics falls under deontological ethics and focuses on the inherent morality of actions themselves rather than their consequences. Moreover, the rights theory of ethics

holds that "respect for human rights are obligatory, regardless of whether they always maximize good" (Schinzinger & Martin, 2000, p. 43). Immanuel Kant, a significant thinker of rights ethics, developed many arguments and theories regarding the right to freedom and the subsequent rights to autonomy, truth, and privacy (Velasquez et al., 2015; Byrd & Hruschka, 2010). It is important to note when considering power dynamics between multiple actors, especially in the context of autonomy, it is important to recognize that there is often an overlap between rights ethics and duty ethics. Duty ethics holds that actions that fulfill our moral obligations to respect the individual's freedom or self-determination are the right actions (Schinzinger & Martin, 2000). For example, it often falls upon the more powerful actor to ensure that the less powerful actor's right to choose freely is upheld. Under these notions, the ethicality of deceitful design is based on whether this practice respects the moral rights of everyone and to the extent that they violate the rights of individuals.

The utilitarian and rights ethical framework analysis is intended to determine a deeper understanding of the societal consequences of obstruction and interface interference in cookie popups. And help aid in the quest of determining good technology and design practices.

Methods

To perform a wholistic and complete ethical analysis, I applied the ethical decision-making framework developed by Sheila Bonde and Paul Firenze (2013) to deceptive cookie popup design. The process included (1) recognizing the ethical issue of dark design patterns, (2) gathering relevant information related to dark design, consent acquisition, and privacy, (3) considering the parties in conflict, and (4) suggesting actions in response to the ultimate ethical consensus under the frameworks of utilitarianism and rights approach.

To obtain relevant information on ethical theories and their application in technology, a systematic literature review was conducted. The literature review focused on key concepts such as privacy, consent, autonomy, and deception, and referred to journal articles that clarified their meanings and significance to humanity and society. Additionally, to gain a nuanced understanding of the ethical concerns surrounding dark design in cookie popups and their effects on relevant parties, scholarly articles that delved into the definition, subtleties, and applications of utilitarian and rights theories of ethics were carefully examined. To acquire a comprehensive understanding of how various actors interact and are impacted by internet cookies, the analysis considers the perspectives, motivations, and objectives of cookie popups and internet application users, internet application designers, the businesses behind the web applications, digital advertisers, and government officials. Furthermore, to ensure the accuracy of concept definitions and information regarding cookie application and usage, I aimed to collect technical resources that were published within the last ten years. Additionally, to direct the focus of the ethical discussion, only two only two specific design strategies, obstruction, and interface interference, were analyzed in more depth.

Overall, this research utilizes a combination of literature review and meta-synthesis to investigate the ethical issues related to the cookie consent forms and design strategies that affect users' autonomy and privacy. The research provides insight into the design strategies that promote ethicality and inclusivity in technology and those that threaten individual freedoms and civil liberties. Furthermore, this analysis offers a contemporary understanding of the ethical issues surrounding the implementation and usability of cookies by focusing on current resources and design strategies.

Analysis

While technology is rapidly developing and being integrated into everyday functions of business, education, and socialization, it is imperative to ensure that users are informed and in control of when their data is being collected, who has access to it, and how it is being used. Otherwise, the current standards of privacy and freedom on the internet are put at risk. The presence of manipulative design strategies in cookie consent popups minimizes the legitimacy of user consent acquisition.

Utilitarianism, a consequentialist ethical theory, suggests that actions are ethical if they lead to the greatest amount of happiness for the most people and do not cause harm to an alternative party. When beginning to apply the utilitarian theory to the ethical dilemma of dark design patterns in cookie popups it is important to take note who is affected by this action. Most obviously, internet applications and their users have a direct role in the design and interaction of these consent forms. However, digital advertisers and data companies also implement their own cookies to collect data or receive user data from cookie collection by the application itself. They use for this data ranges from creating target advertising campaigns for political candidates to research and development.

To organize a utilitarian ethical analysis, the dilemma can be thought about as a balance sheet. On one side of the balance sheet is how the actors in the dilemma are helped and benefited. On the other side is who is harmed by the questionable action. In this case the decision in question is the utilization of dark design patterns in cookie consent popups, not the use of cookies themselves.

Dark design elements in cookie consent popups benefit various actors in the online ecosystem. For users, it encourages their use of allowing all cookies, which can make the

experience of a website more effortless. Such design elements make the initial interface of popups simpler and easier to move past and get to the application quicker. An example could be a popup where there is only one radio button available, and when selected, allows "All Cookies." For businesses and applications, dark design elements allow them to provide a more personalized and fully functional website experience to more users, which leads to increased user retention, more money spent on the site, and more ads viewed, or products bought, generating more wealth for the application. This, in turn, can provide job security and salary for employees and lead to the continuous generation of wealth within the section of the economy the application resides in. Advertisers and data analytic companies also benefit from the use of dark design elements as they coerce users into selecting less privacy-protective options, which provides them with more data points to create target audiences and curated ads. This, in turn, provides individuals with more individualized shopping, viewing, or entertainment experiences.

Ultimately, if dark design, namely obstruction and interface interference were banned from being used in cookie consent forms, these benefits would be lost. However, that may not actually be the case. While many might initially think that requiring internet businesses to account for privacy might make business lose money due to the monetary value of data that could no longer be sold or putting funds and time into creating non deceptive cookie popups and through privacy policies. Consequently, there are case studies that suggest “companies that safeguard their users’ privacy can ‘increase use and consumer spending,’ and ‘generate positive press and create customer loyalty’” (Richards, 2014, p. 33). Similarly, according to Maier and Harr (2020), “customer happiness, trust, and credibility is likely reduced by these deceiving strategies” (p. 191) which may adversely affect a web application’s traffic, profits, and data collected overall. Which would also affect the access third party data companies would have to user data, depending on the

popularity of the web application. Meaning removing deceitful design patterns from their cookie popups and providing users with the tools to accurately determine their privacy would majorly benefit business. Furthermore, as consumers gain awareness of the repercussions of their online activities and are presented with a growing number of choices, they will increasingly require consent interfaces that are not only inventive but genuinely safeguard their privacy. This even presents companies with the chance to innovate and compete by prioritizing privacy protection (Richards, 2014). The benefits of web applications often correspond to the benefits seen by advertisers and data analytic companies, and more significantly if most internet applications took the step to reap the benefits mentioned. Additionally, by protecting user's right to privacy and data collection might also provide president and protect the privacy of the application and third parties (Norberg et al., 2007). Users would benefit from being able to interact with cookie consent popups easily and effectively and give informed consent. The lack of deceitful design elements correlates to a lessoning of coercion and provides more autonomy to the data collection process. These human and personal rights, while not pertinent to utilitarianism, will be revisited later.

Generally, utilitarianism is very subjective as are all ethics, however based on the previous points, the balance sheet seems to suggest that the benefits created from the use of dark design pattern in cookies would not be completely lost in their absence. And perhaps the lack of obstruction and interface interference would promote similar benefits to when they were practiced. Although the division between the benefits and harm caused by deceptive design in cookie consent popups gives a thorough perspective on overall impact on society and the closely related parties, utilitarianism has limitations. As addressed in the literature review, there is significant difficulty in measuring the future implications of data collection and use today (Schinzinger & Martin, 2000; van de Poel & Royakkers, 2011). Data does not disappear after being used once; it is stored and

can be used for various purposes, both legitimate and illegitimate (Richards, 2014). As more people become connected to the internet and share their data, the potential for privacy violations and misuse of personal information increases. It is possible that deceitful cookie popups can compound these consequences by allowing unethical data collection practices to continue unchecked. Additionally, there is some criticism that suggests individual rights should not be sacrificed for the greater good (Schinzinger & Martin, 2000). These alternative theories suggest that everyone has fundamental rights that should be respected, regardless of whether it leads to an increase in overall happiness.

The rights theory posits that individuals have inherent rights that should be protected and respected by society, including the right to privacy, autonomy, and freedom from harm (Velasquez et al., 2015). Any actions that infringe upon these rights are considered unethical. Freedom is an extremely expansive term interpreted varyingly depending on the context and environment. In a broad sense, Byrd and Hruschka's (2010) interprets Kant's idea of freedom as the ability to determine one's own actions without coercion, constraints, or limitation to exercising this choice. Taken further, the right to freedom indicates that a person not only can be their own master but has a claim against those who try infringing upon this autonomy (Burton et al, 2019; Byrd and Hruschka, 2010; Velasquez et al., 2015). When consent forms utilize obstructive and interface interference design elements, users are being punished for having differing preferences from the ones set or made easily accessible by the web application. For instance, if a user must click on multiple links, go to multiple windows, or make multiple selections to deny the use of cookies that user had to sacrifice their time, exert additional effort, or forfeit their access to the service provided by the application. The penalties caused by dark design elements like the previous example coerce users to simply select the most obvious or unobstructive path to the application (Habib et al., 2022;

Maier & Harr, 2020). This unavoidable coercion by the implementation of dark design by the cookie popup interface designer prevents the user from making a voluntary choice regarding their consent and privacy level. Furthermore, if consent is not given voluntarily and freely then it is ultimately not consent, it is rather a means to an end (Machuletz & Böhme, 2020). If a user did not actually consent to the collection of their data via cookies, then the internet application and third parties who own those cookies do not have the right to use or disperse the information collected, since it infringes on the users' right of freedom. And because there are currently applications that utilize cookie data based on the "consent" collected via popups with deceptive design elements, the use of these popups is additionally infringing on a user's right to privacy, defined as the right to determine the collection, use, and release of their personal information. Therefore, breaking every aspect of the rights theory as it relates to freedom and consequently to autonomy and consent (Byrd & Hrushka 2010).

In 2020, Maier and Harr conducted interviews and focus groups where they asked users to interact with websites that utilized deceiving techniques. In this process they discovered that "Although the experience of facing behavior-influencing elements makes some participants want to leave a website completely, it seems as if the benefits that come with using a website or application often outweigh the encountered negative aspects" (p. 187). Internet application business teams are motivated by user interaction and profit and are aware of their value to consumers and use this to their advantage. This power imbalance is mitigated by the implementation of informed consent (Burton et al., 2019). However, the implementation of dark design patterns in cookie popups prevents users from freely giving informed consent. And given that web designers are already creating cookie popups, they can simultaneously make them without dark design elements. Therefore, because of an applications power to infringe on the freedom and

privacy rights of its users via these cookie popups with manipulative elements, and they can change the design of these popups, they in fact have a duty to respect and uphold their uses' autonomy (Byrd & Hruschka, 2010). However, why can't users just put in a little more effort to select their preferred level cookie usage or become more informed about the risks? Why must it be up to the application to provide these features to users? My argument is that humans tend to default to truth, meaning they give the benefit of the doubt unless given sufficient evidence to prove they should think otherwise (Gladwell, 2020). This idea is also supported by Richards' (2014) research regarding privacy, where they argue "Customers share their data with companies under the expectation that it will be treated ethically and responsibly. There is good evidence that consumers share because they think that privacy law is considerably more protective than it really is; for example, that the existence of a privacy policy means that personal information will not be shared or sold to others without their actual consent" (p. 31). Because of this naturally human trait, the duty of accurately providing the risks and giving users the opportunity to legitimately determine if there is enough evidence to reject the use of cookies remains with the web application.

In the case of cookie consent popups, these forms can be seen as an invasion of users' rights to control their personal information. From a rights perspective, websites have a duty to respect these fundamental rights and provide users with clear and meaningful choices to maintain users' autonomy. Otherwise, when users' rights are not respected and protected, there can be serious implications. This can include making people feel unsafe or threatened online and therefore hinder the free exchanging of ideas and information. Many of these implications have yet to be discovered or fully realized due to the newness of the internet and data collection.

Conclusion

While cookies were initially designed to make interacting with websites and advertisements more enjoyable and personalized, there has been a popularized concern regarding the potential for this technology to be exploited because of greed and skewed power dynamics. And if technological designs, including the design of cookie popup interfaces, are supposed to serve the user, it is important to understand design-related ethical implications (Maier & Harr, 2020). While ethics are ever evolving and subjective, the utilitarian ethical analysis brought to light the major harms of deceitful design not only to users, but to internet and data companies. Additionally, under rights ethics, it is shown that web applications that collect users' data via cookies have a duty to not use deceitful design in their consent form interfaces because they ultimately have a duty to protect and uphold the individual rights of people and not inhibit their freedom. These ethical conclusions can serve as guidance for web designers when making decisions about user interface elements and their orientation.

Moreover, this paper can serve as a foundational resource in future research to bolster the case for ethical design, or as a point of reference to corroborate or challenge the ethical conclusions and approaches of other researchers in the field. There is a need for additional research that examines more concretely and quantitatively the consequences of sacrificing privacy for technological advancement, and how it impacts individual freedoms, civil liberties, and livelihood. It is crucial to have an open dialogue on this issue because it is these conversations and created evidence that set the standard for the level of privacy and autonomy internet users are willing to accept.

On a positive note, there is already a push for change within the technology sector to increase inclusivity and ethicality in the design process (Maier & Harr, 2020). New legislation is

being proposed and implemented in the United States to protect user data and privacy, which provides hope that internet users who interact with cookies will remain the priority over the benefit of potential fiscal gain (Kelly, 2018). Overall, the use of cookies and data collection in the digital world has highlighted the need for ethical design practices that prioritize user privacy and autonomy. Further research, dialogue, and the implementation of ethical design practices can ensure that technological advancements do not come at the cost of individual freedoms and civil liberties.

References

Bonde, S., & Firenze, P. (2013). A Framework for Making Ethical Decisions. Brown University. https://www.brown.edu/academics/science-and-technology-studies/framework-making-ethical-decisions#:~:text=The%20Rights%20Approach&text=This%20approach%20stipulates%20that%20the

Brignull, H. (2013). Dark patterns: Inside the interfaces designed to trick you. *The Verge*. https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-totrick-you

Brunton, F., & Nissenbaum, H. (2016). *Obfuscation: A User's Guide for Privacy and Protest*. The MIT Press.

Burton, E., Clayville, K., Goldsmith, J., & Mattei, N. (2019). The Heart of the Matter: Patient Autonomy as a Model for the Wellbeing of Technology Users. *Proceedings of the 2019*

AAAI/ACM Conference on AI, Ethics, and Society, 13–19. https://doi.org/10.1145/3306618.3314254

Byrd, B., & Hruschka, J. (2010). The right to freedom. In *Kant's Doctrine of Right: A Commentary* (pp. 77-93, 294-297). Cambridge: Cambridge University Press. doi:10.1017/CBO9780511712050.005

Cranor L. F. and Habib H. (2023). Metrics for Success: Why and How to Evaluate Privacy Choice Usability. *Communications of the ACM*, 66(3), 35–37. https://doi.org/10.1145/3581764

Dembrow, B. (2022). Investing in human futures: how big tech and social media giants abuse privacy and manipulate consumerism. *University of Miami Business Law Review, 30(3),* 324-349. https://heinonline.org/HOL/Page?handle=hein.journals/umblr30&collection=journals&id=352&startid=352&endid=377

Gladwell, M. (2020). *Talking to strangers*. Penguin Book.

Habib, H., Li, M., Young, E., & Cranor, L. (2022). "Okay, whatever": An Evaluation of Cookie Consent Interfaces. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22) (pp. 1-27). Association for Computing Machinery. https://doi-org.proxy1.library.virginia.edu/10.1145/3491102.3501985

Kelly, M. (2018). How Congress could rein in Google and Facebook. *The Verge*. https://www.theverge.com/2018/10/31/18041882/congress-data-privacy-google-facebook-gdpr-markey-klobuchar

LaCroix, K., Loo, Y. L., & Choi, Y. B. (2017). Cookies and Sessions: A Study of What They Are, How They Work and How They Can Be Stolen. *2017 International Conference on Software Security and Assurance (ICSSA)*, 20–24. https://doi.org/10.1109/ICSSA.2017.9

Lewis, P., Pegg, D., & Hern, A. (2018). Cambridge Analytica kept Facebook data models through US election. *The Guardian*. https://www.theguardian.com/uk-news/2018/may/06/cambridge-analytica-kept-facebook-data-models-through-us-election

Machuletz, D. & Böhme, R. (2020). Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies*. 2020. 481-498. 10.2478/popets-2020-0037. https://petsymposium.org/popets/2020/popets-2020-0037.pdf

Maier, M., & Harr, R. (2020). Dark design patterns: An end-user perspective. *Human Technology, 16*(2), 170-199. https://www.proquest.com/scholarly-journals/dark-design-patterns-end-user-perspective/docview/2681456628/se-2

Mejtoft, T., Frängsmyr, E., Söderström, U., & Norberg, O. (2021). Deceptive design : cookie consent and manipulative patterns. *34th Bled eConference: Digital Support from Crisis to Progressive Change: Conference Proceedings*, 397–408. https://doi.org/10.18690/978-961-286-485-9.29

Minkkinen, M. (2019). Making the future by using the future: A study on influencing privacy protection rules through anticipatory storylines. *New Media & Society*,21(4), 984–1005. https://doi.org/10.1177/1461444818817519

Nielsen, J. (2020). 10 Usability Heuristics for User Interface Design. Nielsen Norman Group. https://www.nngroup.com/articles/ten-usability-heuristics/

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs, 41(1), 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Richards, N. M. (2014). Four privacy myths. *Revised form," A World Without Privacy*. https://ssrn.com/abstract=2427808

Schinzinger, R., & Martin, M. W. (2000). Utilitarianism, Rights Ethics, and Duty Ethics. In *Introduction to Engineering Ethics* (pp. 41-47). *United States of America: McGraw-Hill Higher Education.*

Sit, E., & Fu, K. (2001). Inside Risks: Web cookies: Not just a privacy risk. *Communications of the ACM, 44*(9), 120. https://doi.org/10.1145/383694.383714

van de Poel, I., & Royakkers, L. (2011). Normative Ethics. In *Ethics, Technology, and Engineering* (pp. 67–108). Blackwell Publishing.

Velasquez, M., Andre, C., Shanks, T., S J, & Meyer, M. J. (2015). Thinking Ethically. www.scu.edu website: https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/thinking-ethically/#:~:text=The%20virtue%20approach%20to%20ethics