The Facebook-Cambridge Analytica Scandal: Technological Politics and the Design of User Consent

STS Research Paper
Presented to the Faculty of the
School of Engineering and Applied Science
University of Virginia

By

Emmie Halter

February 26, 2025

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.

Nada Basit, Professor, Department of Computer Science

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

Introduction:

In 2018, news broke of an alleged "breach" on Facebook that resulted in 87 million users' profiles being harvested and sold by Cambridge Analytica to various right-wing campaigns, specifically the 2016 Trump Campaign. In the digital age, social media platforms like Facebook play a significant role in shaping online interactions, personal identity, and data privacy. The Cambridge Analytica scandal revealed how Facebook's privacy measures prioritized corporate interests over user protection. Additionally, the scandal highlighted how social media can be easily manipulated to sway election results. In the case of the Cambridge Analytica scandal, the harvested data was used to create "micro targeted advertisements," which were displayed to millions of Facebook users. As was stated by *The Observer*, "the company had harvested millions of Facebook profiles of US voters, in one of the tech giant's biggest ever data breaches, and used them to build a powerful software program to predict and influence choices at the ballot box" (Cadwalladr, 2018, March 20).

The scandal raised questions about data privacy, international digital laws, and Facebook's security practices, but most scholars failed to acknowledge the contribution Facebook itself had to the scandal, specifically surrounding its user interface. The platform's UI design included misleading consent waivers, default privacy settings, and complex language that resulted in limited user autonomy and facilitated the exploitation of personal data through third-party data sharing.

By applying Langdon Winner's framework of *Technological Politics*, which says that technological artifacts can embody specific forms of power and authority, this paper argues that Facebook's user interface disempowered users and made them vulnerable through a technical design that reinforced corporate control over user data, impeded democratic participation, and

limited informed consent. To support my conclusions, I draw on several sources, including academic analyses of the Cambridge Analytica scandal, regulatory reports, user interface studies, and expert discussions on data privacy and platform design.

Literature Review:

Several scholars have studied the ethical issues surrounding the Facebook Cambridge Analytica data scandal, particularly concerns about data privacy and government regulation. While these studies offer useful insights into how personal data was misused and why stronger rules are needed, they often fail to examine how Facebook's design choices made it easier for these breaches to happen. There is also little research on how these design decisions affect users' ability to make informed choices about their data. As a result, there is still a need for a more complete analysis that connects the flaws in user consent systems to their larger impact on society.

In *Cambridge Analytica's Black Box*, Hu (2020) criticizes how the Federal Trade Commission (FTC) handled the scandal, arguing that the $5 billion fine against Facebook didn't address the deeper issues behind data privacy violations. Hu stresses that stronger legal protections are needed to prevent similar problems in the future, saying that the scandal "focuses attention on the need to explore the potential for embedding due process-type inquiries and protections within the enforcement actions by regulatory agencies such as the FTC" (Hu, 2020, p.2). She also points out that Facebook's data policies are so complex and vague that users often have no real understanding of how their information is being accessed, leaving them with little control. Additionally, Hu argues that government agencies don't have the right expertise or enforcement power to properly regulate companies like Facebook. While she does a good job of highlighting problems within regulation, her analysis doesn't explore how Facebook's own

design choices, such as confusing privacy settings, and poorly designed consent waivers, made it easy for companies like Cambridge Analytica to take advantage of users.

Similarly, in *The Cambridge Analytica Affair and Internet-Mediated Research*, the authors focus on the ethical issues of collecting data from social media. They note that "the latest Facebook data breach highlights the need for guidelines for internet-mediated big-data research" (Schneble et al., 2018, p.1). They emphasize that ethical research practices, such as getting clear user consent and minimizing the amount of data collected, should be applied to social media research just as they are in traditional studies. Additionally, they also acknowledge that current regulations don't fully account for the scale and complexity of online data collection, as well as highlight the problem of data being repurposed for uses that people never agreed to. Their study reveals a major gap between the rules that exist and the actual risks users face when their data is collected on a large scale, however, they don't go into detail about how companies like Facebook intentionally design their platforms to confuse users on what they are agreeing to.

While both studies address critical aspects of data privacy and regulatory responses, they do not fully explore the intentional design strategies that may confuse consent processes. My paper aims to address this aspect of the case by critically analyzing how specific design choices in user consent mechanisms such as default settings, interface complexity, and misleading language affect user autonomy and contribute to ethical breaches like the Cambridge Analytica scandal.

Conceptual Framework:

This analysis employs the framework of "Technological Politics," which examines how technological artifacts embody and enact power dynamics and political agendas. By applying this framework, the study focuses on how the design of user consent mechanisms reinforces

particular power structures and potentially marginalizes users. This approach facilitates a new understanding of the intersection between technology design, user agency, and ethical responsibility in the digital age.

Technological Politics is an STS framework that was outlined by Langdon Winner in his influential article *"Do Artifacts Have Politics?"* which explores the relationship between technological systems and power dynamics in society. At its core, Technological Politics challenges the assumption that technology is neutral and instead argues that “the adoption of a given technical system unavoidably brings with it conditions for human relationships that have a distinctive political cast" (Winner, 1980, p. 128). Additionally, Winner emphasizes the intentionality behind the way technologies are implemented which can lead to authoritarian control or democratic participation. In some instances, technologies are purposefully designed to reinforce existing power structures, embedding explicit biases into their functionality. In other cases, biases emerge indirectly, shaped by the implicit assumptions of designers and broader societal influences. Ultimately, Technological Politics provides a critical lens for understanding how technological systems are active agents in shaping social hierarchies, governance structures, and the distribution of power in society.

In the following analysis, I will examine the Facebook Cambridge Analytica case within the framework of Technological Politics. This study highlights how the scandal exemplifies the broader issue of confusing user interfaces and misleading consent agreements, which results in a lack of data privacy. Rather than being an isolated incident, it reflects persistent challenges in regulating digital platforms and ensuring transparency in data governance. Through the lens of Technological Politics I will critically examine Facebook's interface design and its impact on

user consent, as well as the role that data sharing with third parties plays in discussions on privacy rights and digital ethics.

Analysis I : Facebook User Interface Flaws

Facebook's platform is inherently built to favor the company's interests. Whether this involves targeted advertising, curated feeds, or deceptive interface designs, the Facebook programmers have been instructed to include or deny certain features in order to facilitate profit and popularity for the platform. While one could argue that any smart business would do the same thing, Facebook's decisions have resulted in manipulation and exploitation of its users' and their private data. These design choices, as understood through Technological Politics, are not neutral but actively reinforce Facebook's dominance, embedding power structures that prioritize control and company benefit over user autonomy and informed consent.

Facebook's privacy permissions were deliberately vague, making it difficult for users to fully understand how their data would be used. This can be seen in the statement of Frances Haugen, a former Facebook employee, who stated to the Senate, in a public hearing, that Facebook's leadership was aware of the harms caused by its platform but chose to prioritize profits over transparency and user safety. Haugen's role as an insider lends credibility to her claims, especially because she accessed internal research and decision-making records. Her testimony underscores that these weren't accidental design flaws but deliberate choices made at the highest level of the company. She emphasized that Facebook intentionally misled the public and regulators about the extent of its data practices, including how personal information was shared with third parties. She further testified that the company's internal research demonstrated the negative effects of its platform, such as the spread of misinformation, harm to children, and

the facilitation of divisive content, yet Facebook failed to take meaningful action to address these issues (Haugen, n.d.).

Facebook's physical interface further pushed this agenda, by employing "Dark Patterns" in their UI to subtly nudge users into making choices that favor the company's interests. Dark Patterns "utilize knowledge about human psychology in combination with usable design to create deceiving design practices, which do not have the user's interests in mind" (ACM Digital Library, n.d., p.1). An example of this can be seen in a study done by Thomas Mildner and Gian-Luca Savino, two researchers at the University of Bremen. Upon evaluation of Dark Patterns within Facebook's interface it was found that Facebook "moved the logout button and privacy settings into drop-down menus, which can be classified as interface interference [14]. The subtle relocation of core settings is not just a minor inconvenience, it reflects an intentional use of UI design to limit user agency. These buried features make it harder for users to exercise control over their data, and the choice to obscure them suggests an effort to ensure more passive data collection. Given that "Facebook directly benefits from users not logging out (by being able to track them across the web as long as they are logged in), this can be a conscious choice to limit discoverability and thus prevent certain user actions (i.e. logouts)" (ACM Digital Library, n.d., p.3). This is just one example of the deceptive interface designs Facebook employed, which resulted in millions of their users' unknowingly sharing data with third parties such as Cambridge Analytica. The decision to bury logout buttons and privacy settings within a drop-down menu reflects the principles of Technological Politics, where design choices are deliberately made to serve the interests of the creator (Facebook) while taking advantage of the user.

Finally, Facebook sets the default privacy settings to the least restrictive option possible, leaving it to the user to turn these privacy controls on themselves. In his hearing with the U.S. Securities and Exchange Commission, Mark Zuckerberg addressed concerns about Facebook's privacy settings, stating: "If I'm sharing a photo and it can go in my friend's news feeds that's colloquially what I'm referring to as sharing with your friends. But I believe we've also had a control so that way in people's privacy settings, they could turn off the ability for information that they shared with their friends to be used in other developer's apps" (U.S. Securities and Exchange Commission, n.d., p.42). This design choice forces the users to search for privacy controls, which as has been previously said are purposefully difficult to find, and turn the adequate privacy settings on themselves. If Facebook was designing their platform in the interests of their users, they would have these settings already programmed to be on the most private option, and then provide an opt-in, opt-out choice for data sharing. Furthermore, the lack of clarity and confidence in Zuckerberg's response demonstrates that not even him, the founder of Facebook, is aware of the nuances of the platform's privacy controls. Once again, Facebook's platform demonstrates how technology can be used to take advantage of certain groups, due to their lack of control and knowledge, while benefiting other groups who wield more societal power. By diminishing users' autonomy, Facebook strengthens its control over its revenue and business model, often at the expense of others.

As has been discussed above, Facebook has employed several manipulative ways to retrieve their users data, sacrificing both user privacy and autonomy. While some arguments could be made that Facebook collects user data to give users a more personalized Facebook experience with ads and posts targeted towards their interests, it should still be noted that these justifications ignore the ethical implications of a deceiving UI design. A prominent example of

this, is the way Facebook's targeted advertising has enabled small businesses to expand their reach and attract more customers. With users implicitly consenting to certain data practices, small businesses have been able to leverage Facebook's vast data collection to refine their marketing strategies, ensuring their advertisements reach the most relevant audiences. Sheryl Sandberg, former Facebook COO, said in an interview with Forbes that: "The technology is democratizing …Your phone can shoot a video ad, and for just a few dollars, you can reach people on Facebook. The fact that those tools are now simple enough and accessible enough that 5 million can use them is pretty exciting" (Chaykowski, 2017). While Sandberg frames the platform as a tool for empowerment, this quote also highlights a key tension: the same tools that enable small businesses to flourish are built on opaque data practices that most users don't fully grasp. The trade-off between business growth and user privacy is presented as neutral, but it's far from ethically straightforward. The practice of data collection presents a significant benefit and should not be overlooked. Facebook has contributed to economic growth and supported the success of small businesses, which is a pillar in American society. However, while these advantages are significant, they do not justify the ethical implications of Facebook's manipulative design choices.

The company has faced scrutiny over its handling of user consent and privacy, particularly in how it hides the extent of its data sharing practices. The Federal Trade Commission (FTC), in its $5 billion settlement with Facebook following the Cambridge Analytica scandal, highlighted these concerns. They stated that "the Department of Justice will file a complaint on behalf of the Commission alleging that Facebook repeatedly used deceptive disclosures and settings to undermine users' privacy preferences in violation of its 2012 FTC order. These tactics allowed the company to share users' personal information with third-party

apps that were downloaded by the user's Facebook "friends." The FTC alleges that many users were unaware that Facebook was sharing such information, and therefore did not take the steps needed to opt-out of sharing" (Federal Trade Commision, 2019). Facebook's ability to create the illusion of user control while continuing to share their data highlights how technology can be designed to empower one group while diminishing another. This further emphasizes how Technological Politics can be applied to this case, as these interface decisions are not merely technical but deeply political, reinforcing Facebook's control over its customers by limiting user agency while prioritizing the company's financial and strategic interests.

Analysis II : Data Sharing with Third Parties

In addition to misleading interfaces that denied users full autonomy of their data within Facebook, the platform also allowed third parties to exploit their users' data without consent. In the case of the Cambridge Analytica (CA) Scandal, CA was able to procure massive amounts of Facebook data, even from private accounts, due to a loophole in Facebook's API. The loophole "allowed third-party developers to collect data not only from users of their apps but from all of the people in those users' friends network on Facebook" (Romano, 2018). This was a very avoidable circumstance, but was not addressed by Facebook until 2015 when they changed their "third-party API to block access to the kind of massive data sets that Cambridge Analytica was collecting" (Romano, 2018).

Many reports initially described this data sharing as a leak, but it has since been established that it was intentional, with Facebook knowingly granting mobile developers access to this data. The CA mastermind behind this operation was Aleksandr Kogan, a data miner originally from Russia who moved to the U.S. when he was seven and attended college at UC Berkeley. Kogan developed a personality quiz app called "This Is Your Digital Life," which

collected data not only from users who installed it but also from their Facebook friends, resulting in the procurement of up to 87 million profiles. What makes this number particularly concerning is that most of these users never directly interacted with the app. The data of friends of users was silently collected, which demonstrates just how far-reaching Facebook's ecosystem of consent truly was. He later provided this data to CA, which used it to create targeted political advertising during the 2016 U.S. presidential election.

In 2018 a former CA employee came forward, Christopher Wylie, and explained the deceptive work that was done behind the closed doors of CA offices. Wylie states, "Facebook could see it was happening,"..."Their security protocols were triggered because Kogan's apps were pulling this enormous amount of data, but apparently Kogan told them it was for academic use. So they were like, 'Fine'." (Cadwalladr, 2018, March 17). Even though Facebook knew about the data sharing, they made no effort to investigate how it was being used. This suggests that they prioritized their relationship with CA and political interests over protecting their users. Furthermore, it highlights how technology and politics are becoming more connected, with data mining and targeted ads playing a big role in shaping public opinion and elections.

The Cambridge Analytica scandal serves as a clear example of how social media platforms can be exploited for political gain, raising serious concerns about data privacy and election integrity. Facebook's failure to prevent or properly investigate the misuse of user data demonstrates a disregard for user privacy, prioritizing business and political relationships over ethical responsibility. The European Parliament has acknowledged this negligence, stating that Facebook entered into agreements with developers without ensuring compliance with data protection laws, leading to significant consequences (European Parliament, 2018, p.5). In response to such violations, there have been calls for stronger regulations to prevent future

abuses. One recommendation suggests that third party audits should be mandatory after political campaigns to confirm that personal data has been deleted or that proper consent was obtained before any data sharing occurred (European Parliament, 2018, p.10). These recommendations reflect a growing recognition of the need for stricter oversight in the digital space, ensuring that powerful platforms like Facebook are held accountable for their role in safeguarding user information. As technology and politics continue to intersect, regulatory measures will be crucial in protecting democratic processes and preventing data exploitation for political manipulation.

Conclusion:

The Facebook-Cambridge Analytica scandal demonstrated how deeply intertwined technology is with society and how digital platforms can significantly shape public opinion, particularly in political contexts. Through the lens of Technological Politics, this case reveals that Facebook's interface design choices, such as vague consent agreements, default privacy settings favoring data collection, and dark patterns, were not merely technical decisions but deliberate design choices to maximize data collection and profit. These interface manipulations not only facilitated data exploitation but also obstructed users' ability to make informed decisions about their personal information.

Additionally, Facebook's lenient data sharing policies enabled third parties, such as Cambridge Analytica, to harvest vast amounts of user data under the assumption of academic research. The scandal underscored the dangers of unchecked corporate influence over digital spaces, demonstrating how social media can be weaponized for political manipulation. Despite regulatory fines, the incident highlighted persistent gaps in digital governance, where legal frameworks struggle to keep pace with evolving technological landscapes.

Ultimately, this case serves as a cautionary tale about the ethical responsibilities of tech companies in the digital age. Moving forward, stronger regulations, greater transparency, and more user-centric design choices are necessary to protect individual privacy and ensure that digital platforms do not become tools for political and corporate exploitation. As technology continues to evolve, its political and ethical implications must remain at the forefront of discussions on data privacy, digital rights, and platform accountability.

References

ACM Digital Library. (n.d.). *Cambridge Analytica and Facebook: The scandal and its aftermath.* Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). *'I made Steve Bannon's psychological warfare tool': Meet the data war whistleblower.* The Guardian. https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

Cadwalladr, C., & Graham-Harrison, E. (2018, March 20). *Cambridge Analytica suspends CEO Alexander Nix*. The Guardian. https://www.theguardian.com/uk-news/2018/mar/20/cambridge-analytica-suspends-ceo-alexander-nix

Chaykowski, K. (2017, April 10). *Sheryl Sandberg: Facebook hit 5 million advertisers by turning users into marketers*. Forbes. https://www.forbes.com/sites/kathleenchaykowski/2017/04/10/sheryl-sandberg-facebook-hit-5-million-advertisers-by-turning-users-into-marketers/

European Parliament. (2018, October 25). *European Parliament resolution of 25 October 2018 on the use of Facebook users' data by Cambridge Analytica and the impact on data Protection.* https://www.europarl.europa.eu/doceo/document/TA-8-2018-0433_EN.html

Federal Trade Commission. (2019, July 24). *FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook.* https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

Haugen, F. (n.d.). *Testimony before the U.S. Senate Committee on Commerce, Science, and Transportation.* U.S. Senate. https://www.commerce.senate.gov/services/files/FC8A558E-824E-4914-BEDB-3A7B1190BD49

Hu, M. (2020). Cambridge Analytica's Black Box. *Big Data & Society, 7*(2), 1–5. https://journals

.sagepub.com/doi/10.1177/2053951720938091

Romano, A. (2018, March 20). *The Facebook data breach, explained.* Vox. https://www.vox.com /2018/3/20/17138756/facebook-data-breach-cambridge-analytica-explained

Schneble, C. O., Elger, B. S., & Shaw, D. (2018). The Cambridge Analytica affair and Internet-mediated research. *EMBO Reports, 19*(8), e46579. https://www.embopress.org /doi/full/10.15252/embr.201846579

Winner, L. (n.d.). *Do artifacts have politics?* Georgia Institute of Technology. https://faculty.cc.gatech.edu/~beki/cs4001/Winner.pdf

U.S. Securities and Exchange Commission. (n.d.). *Mark Zuckerberg testimony transcript.* https://www.sec.gov/files/zuckerberg-transcript.pdf