Facebook Data Breach of 2018 Examined through Care Ethics

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

By

Shivani Surti

April 10, 2022

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.

Signed: _____

Approved: _____ Date _____
Benjamin J. Laugelli, Assistant Professor, Department of Engineering and Society

Introduction

In 2014, Aleksandr Kogan created a personality quiz app called “thisisyourdigitallife” on Facebook’s platform, funded through Cambridge Analytica. The app had access to the user's personal information as well as data on all the friends they had added to the app. Four years later, through a series of press releases and interviews performed by Christopher Wylie, it was discovered that Cambridge Analytica was leveraging user information to create personalized ads to manipulate Facebook users (Rehman, 2019). Many scholars usually blame Facebook’s lack of user privacy protection as being the root of the issue. They believe that Facebook could have resolved this issue by having better privacy policies.

However, this interpretation fails to consider Facebook’s lack of transparency to its users. Facebook, in fact, did have many privacy settings in place that users could use to protect themselves and control how much of their information is stored by apps and Facebook. Neither did the users not know that these settings existed, nor did they know about the risks involved in not protecting their data (Kozlowska, 2018). Suppose we continue to limit the understanding of the problem to just a lack of privacy policy. In that case, scholars fail to comprehend Facebook’s inability to provide transparency for its users, which contributed to the data breach.

I will analyze Facebook’s actions before and after the Cambridge Analytica data breach through the lens of care ethics to determine the morality of Facebook in the Cambridge Analytica data breach. I will use Tronto’s four stages of care: attentiveness, responsibility, competence, and responsiveness, to evaluate Facebook’s actions. Finally, I will show that Facebook’s actions were immoral and hindered its relationship with its users by leveraging interviews given by Wylie, Facebook’s official posts regarding the issue, and journal articles written by scholars.

Literature Review

The scholarly literature surrounding the Facebook Data Breach of 2018 is primarily concerned with user privacy. It primarily focuses on how Facebook could have done a better job protecting user information; however, it fails to recognize the relationship between Facebook and its users. Facebook's lack of care and transparency resulted in users losing their trust in the product and hurting the relationship.

In Ikhlaq ur Rehman's journal, *Facebook-Cambridge Analytica data harvesting: What you need to know*, he argues that Facebook has never been considerate of user privacy. In fact, the entire model of Facebook's development is based on commercialization. Facebook stores all the generated user data to run targeted advertisements. A significant security threat was through the applications that were hosted on Facebook. These applications include apps such as Farmville, Texas HoldEm Poker, and the "thisisyourdigitallife" personality app. These applications had access to the user's information who was using the application and data on all the friends they had added to the app. This means that if one application was wrongfully taking data from a user, a person who was simply friends with this user could also be exploited. Rehman discusses the different approaches that Facebook took to prevent a situation like the exploitation of 2018 from happening again. He does, however, criticize Facebook's lack of attention to this matter from the beginning (Rehman, 2019). While Rehman does a great job of breaking down the case regarding the invasion of user privacy, he fails to consider Facebook's relationship with its users. There is no emphasis on how Facebook's lack of care for its users caused them to lose their trust in Facebook.

In *Cambridge Analytica's black box*, Margaret Hu investigates what happened with the data that was exploited from 87 million users on Facebook without their consent. At the time, the

Presidential Elections were around the corner, and the demand for attracting voters was high. According to the creator of the "thisisyourdigitallife" app, the app adhered to all the guidelines that Facebook had when the app was available to the public. Due to Facebook's loose policies, Aleksandr Kogan gathered detailed information about users and their friends through the personality quiz app and their profiles. Not only was this information collected, but Facebook once again used it to display personalized ads that will attract a user to vote for a particular political party, invading a user's privacy (Hu, 2020). Like Rehman, Hu does a great job analyzing the flaws within Facebook's system that allowed Cambridge Analytica to exploit user privacy. However, he fails to consider the lack of transparency and care that Facebook displayed by violating the user's trust and not protecting the user's privacy. Both Rehman and Hu analyze Facebook's actions through the lens of Facebook's flawed user privacy policies but do not take the time to explore the impact of Facebook's loose data privacy policies on the relationship Facebook has with its users.

Privacy is becoming a more prominent issue as the number of social media platforms increases, with the Cambridge Analytica case being a prime example. While both scholars argue that Facebook mishandled user information, they fail to take a broader look into Facebook's relationship with its users. By limiting their understanding and argument to just Facebook's user privacy flaws, the scholars fail to see the bigger picture. They forget that Facebook and the users have a relationship that requires transparency. Users were not informed about the risks involved with the user privacy policy and trusted Facebook. My analysis will focus on how Facebook treated its users before and during the rise of this issue. Before that, I will review the ethical framework I will be using to evaluate Facebook's morality in the Cambridge Analytica case.

Conceptual Framework

Using Care Ethics, the morality of the actions taken by Facebook during the Cambridge Analytica data leak scandal can be evaluated. Care ethics does not stress universal moral principles; instead, it values relationships. According to care ethics, one does not learn about morals through general ethical principles but by seeing people show emotions towards other people. A moral problem is solved in care ethics by maintaining relationships with other people. Care ethics places tremendous importance on the concept of connectedness; it allows a person to show and feel empathy towards another person. The amount of care that a person should show depends on their role (van de Poel & Royakkers, 2011).

Sander-Staudt defines *care* as "a practice, value, disposition, or virtue, and is frequently portrayed as an overlapping set of concepts." Care is displayed by understanding other people's vulnerabilities and knowing what correct or incorrect action is to take at that time—using this information on people's vulnerabilities as a way to show empathy and build relationships. The actions taken in building that relationship are contingent on the amount of empathy another person has (Sander-Staudt, 2022).

Joan Tronto breaks care into four sub-categories: attentiveness, responsibility, competence, and responsiveness. These four sub-categories help to determine whether an ethical action was taken (Klaver & Baart, 2011). The first step towards care is attentiveness. Tronto defines *attentiveness* as the "quality of individuals to open themselves for the need of others." The next step, *responsibility*, is "a willingness to respond and take care of need." *Competence* is "the ability to provide good care," and *responsiveness* is to "understand the needs of others and actively see the potential of abuse in care" (Sander-Staudt, 2022).

Ultimately, Facebook's actions can be evaluated in accordance with the four sub-categories of care. By analyzing the relationship between Facebook and its users using Facebook and Cambridge Analytica interviews, Facebook's official posts, congressional hearings, and journal articles written by scholars, we can determine the moral standings of its privacy guidelines.

Analysis

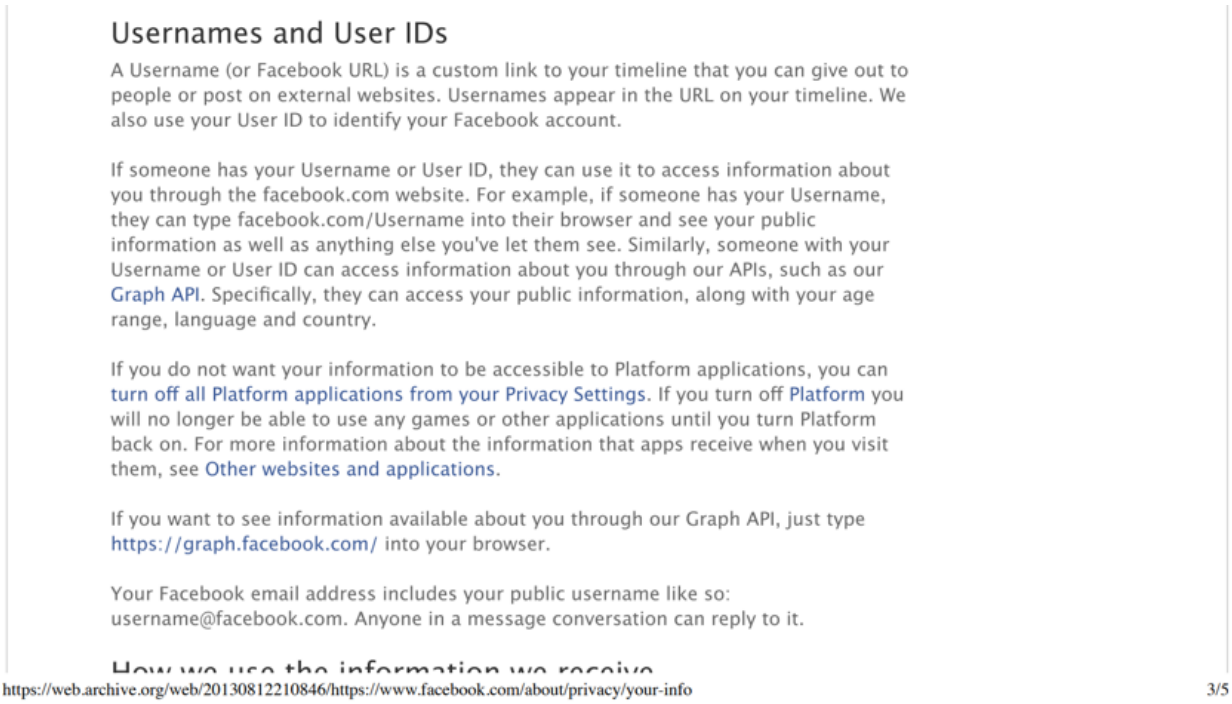
I will be breaking down Facebook's actions in the wake of the Cambridge Analytica data breach to determine Facebook's morality using care ethics. I will use the four stages of care ethics: attentiveness, responsibility, competence, and responsiveness. By evaluating each of these sub-categories, I will be able to determine whether Facebook's actions in the relationship were moral or not.

Attentiveness

The first stage of care is attentiveness; it is becoming aware of others' needs. Failing to show attentiveness to its users meant that Facebook failed to show appropriate care within the relationship. Here I will review whether Facebook showed attentiveness to its users' needs during the Cambridge Analytica scandal.

As established, Facebook and its user base have a relationship that does require care. The question becomes whether Facebook was aware of the user's need for care. During the Cambridge Analytica scandal, transparency was the primary need for care as the users did not know that their data was leaked. Users were not informed of Facebook's business model nor how their information will be used.

Facebook does have privacy settings that a user can use to protect their data. These settings are not user-friendly. They are lost in the other user settings, difficult to find. The privacy policy itself is very long or very technical, resulting in a lack of transparency:



Usernames and User IDs

A Username (or Facebook URL) is a custom link to your timeline that you can give out to people or post on external websites. Usernames appear in the URL on your timeline. We also use your User ID to identify your Facebook account.

If someone has your Username or User ID, they can use it to access information about you through the facebook.com website. For example, if someone has your Username, they can type facebook.com/Username into their browser and see your public information as well as anything else you've let them see. Similarly, someone with your Username or User ID can access information about you through our APIs, such as our Graph API. Specifically, they can access your public information, along with your age range, language and country.

If you do not want your information to be accessible to Platform applications, you can turn off all Platform applications from your Privacy Settings. If you turn off Platform you will no longer be able to use any games or other applications until you turn Platform back on. For more information about the information that apps receive when you visit them, see Other websites and applications.

If you want to see information available about you through our Graph API, just type https://graph.facebook.com/ into your browser.

Your Facebook email address includes your public username like so: username@facebook.com. Anyone in a message conversation can reply to it.

How we use the information we receive

Figure 1. **A snapshot of the Data Use Policy section of the Privacy Policy** - In this snapshot, general information is shown to the user on how someone can access their profile information (Data Use Policy, 2013)

Facebook's privacy policy in 2013 was split into different policy pages for user convenience. Figure 1 is a small section of the Data Use Policy page. Two key components of this figure are the technicality of the terms and the number of pages. The "Usernames and User IDs" section refers to the Graph API; however, the average user has no idea what an API is nor its purpose. There is little information on the page itself to give users a brief understanding. This section even goes in-depth about how other users can use Facebook's URL to access their profiles. While this is valuable information to know, this is too technical for the average audience. Taking a closer look at the length of just the Data Use Policy, it is a total of 5 pages.

According to a study, users spend about 10-20 seconds on a webpage (Nielsen, 2011). With a total of 5 pages being just the Data Use Policy, which is rampant with technical terms that the average audience would not understand, users are not interested in attending to the privacy policy. Thus, users agree to these privacy policies as they trust Facebook to protect their data.

Some may argue that it is the user's responsibility to understand what they are signing up for. Facebook did explicitly state in its privacy policy how user information is used and what steps users can take to protect their data. However, it is important to consider that Facebook never considered users when crafting their privacy policy.

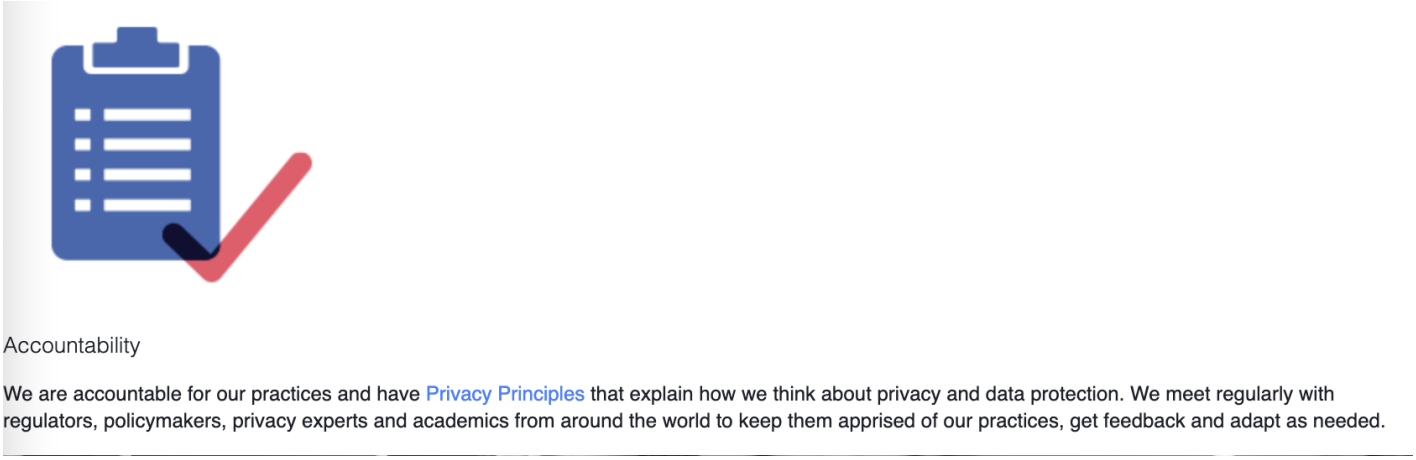


Figure 2. A Screenshot of Facebook's GDPR Statement - This screenshot displays a section of the principles that Facebook vows to follow as a proactive step in response to the Cambridge Analytica case (General Data Protection Regulation (GDPR), 2018)

A statement was released by Facebook accepting the General Data Protection Regulation worldwide post the Cambridge Analytica data breach through its Facebook Business site. The above figure is a snapshot of a section of the website Facebook created. The key piece of information here is that "we meet regularly with regulators, policymakers, privacy experts, and academics." Nowhere in this statement did Facebook consider the people actually reading and being affected by its privacy principles. While it is good to learn and stay up to date on privacy measures, it is also important for users to understand the measures put into place. The average

user is not included in the feedback process; however, they are the ones being affected. This statement was released post the Cambridge Analytica data breach, where Facebook became aware of (if not previously) the lack of transparency they were showing to the users. Even while acknowledging this, Facebook continued the practice of leaving users out of the discussion on privacy matters and did not consider creating a user-friendly approach to explaining the privacy policies.

Users did not know they needed to check user privacy settings before the Cambridge Analytica scandal. The lack of transparency by Facebook to establish to its users the risks involved in not setting user privacy showed a lack of care. In the wake of the Cambridge Analytica data breach, users recognized the need to protect personal information. Facebook did have pre-set privacy settings that were not private at all. Facebook's entire business model is centered around targeted user ads. They rely on app developers to access user information that can send targeted ads to users. This business model conflicts with user privacy interests (Kozlowska, 2018). By displaying a lack of transparency and awareness for users, Facebook failed the first stage of care; attentiveness.

Responsibility

The second stage of care is responsibility; it considers others' needs as your duty. In this phase, actions taken in the wake of the Cambridge Analytica scandal will be analyzed. The steps that Facebook took will be evaluated based on whether Facebook considers the users' needs, which is transparency for this case.

2015 was when Facebook first learned about the data breach when Facebook's algorithm got triggered by Alex Kogan (the developer of the app) pulling substantial amounts of user data (Cadwalladr, 2018). This was three years before the breach was known to the public by press

releases. In 2016, Facebook removed the “thisisyourdigitallife” app and demanded that Kogan and Cambridge Analytica delete all users' information gathered from the app. Not only did Facebook wait a year before acting, but none of the users that had their information breached were informed about this. Facebook did not even reach out to the Federal Trade Commission about this violation of privacy by Cambridge Analytica (Curtis, 2018). Facebook knew that user information was being collected and used against users via ads without their consent. Still, instead of publicly stating this information to their users, they decided to deal with the matter internally (Hopping & Pro, 2018). By not being transparent about this discovery to the users, Facebook broke users' trust, thus hindering their relationship.

Further, Christopher Wylie, a Cambridge Analytica employee, revealed to *the Guardian* that Facebook did not check whether user data had been deleted. In an interview with Carole Cadwalladr, Wylie described this experience as

> I already had. But literally all I had to do was tick a box and sign it and send it back, and that was it, says Wylie. Facebook made zero effort to get the data back. (Cadwalladr, 2018, p. 20)

I would like to break this statement apart and focus on “all I had to do was tick a box.” This is tremendously important as it shows the amount of care and attention Facebook provides to its users. Instead of ensuring all data was deleted and user privacy was secured, Facebook placed its trust in Cambridge Analytica to follow through with the request. Even while knowing Cambridge Analytica’s actions and company objectives, instead of preserving the relationship between Facebook and its users, Facebook chose to prioritize its relationship with Cambridge

Analytica, disregarding the trust that users showed in Facebook. All of this was handled internally, meaning that the users had no idea that this was happening in the background.

Acknowledging Facebook's actions, Facebook fails to meet the requirements for the second phase of care: responsibility. By not being transparent to the users and not taking appropriate action to provide the care that users needed, Facebook hindered its relationship with users. Facebook decided to handle matters internally to preserve public perception instead of showing its commitment to its users.

Competence

The third stage of care is competence; it provides good and successful care. This phase judges the actions taken in the responsibility phase through the lens of morality. I will examine how Facebook responded to its users and improved in response to the data breach scandal.

As established in the responsibility section, Facebook did not do enough to ensure that user privacy was protected when they first discovered the Cambridge Analytica data breach. Although Facebook demanded certifications from Kogan and Cambridge Analytica to ensure that all user data had been deleted, Facebook did not do a respectable job of enforcing this. It was later understood that Cambridge Analytica still had access to all the data. Furthermore, Facebook was not transparent with the issue to users, showing a lack of care for the relationship and trust users had with Facebook.

Facebook used legality to defend itself by claiming that a data breach had never occurred. According to the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), "data breach" is defined as

> Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed (ISO/IEC 27040, 2022, p. 1).

I would like to point out the most critical word in this definition, “unlawful.” All the data that was gathered by the app was done legally. The app developer did not violate any of Facebook’s rules, nor did they access more information than they were allowed to. The app users also gave consent for their data to be accessed. The real issue is the misuse of the data by Cambridge Analytica (Kozlowska, 2018). While Facebook could escape this case in terms of legality, this is a violation of trust in the lens of care ethics. Facebook failed to show enough care to its users to protect them and ensure that this does not happen.

Even while defending themselves in terms of legality, Facebook did understand that this incident caused many users to lose their trust in the company. To make amends, Facebook took the initiative to update its privacy policy. First, large apps will be monitored and checked for potential privacy violations, and impacted users will be contacted. Second, to eliminate the problem from the root, Facebook will limit the data that app developers can have access to in the first place. If app developers want access to more data, they must get permission from Facebook and the consent of the users. Third, users will be able to decide which apps can have access to their data and manage how much data they are willing to provide. This will be carried out by having a tool on top of their news feeds for easier visibility, as this option was available previously under the privacy settings (Zuckerberg, 2018).

While Facebook has put in efforts to remediate this issue and gain users' trust back, these actions should have been taken earlier to ensure users' privacy. Trying to increase the visibility of

privacy tools does not eliminate the need for transparency to users. Users should be able to know what they are signing up for beforehand. There needs to be more visibility on how user information is used, not just by developer apps but by Facebook itself. Facebook fails the third stage of care, competence.

Responsiveness

The fourth and final stage of care is responsiveness; it is receiving care well. This phase highlights potential abuse in care and how it should be proactively dealt with within the relationship. There has been a debate about reaching a balance between short and long privacy policies for users on social media. Facebook's current privacy policy is extensively long and sometimes too technical for the average audience. Facebook employs many lawyers and engineers to produce the perfect legal privacy policy; however, it is not designed for the user who will be using the product. Instead of taking a defense-first perspective for legality, Facebook should have made their privacy policy for the users and informed them about the risks involved in sharing their personal data (Kozlowska, 2018).

In the wake of the Cambridge Analytica scandal, Facebook released a statement that it will now adhere to the EU General Data Protection Regulations worldwide (Hopping & Pro, 2018).

ZUCKERBERG: Senator, I think everyone in the world deserves good privacy protection. And, regardless of whether we implement the exact same regulation, I would guess that it would be somewhat different, because we have somewhat different sensibilities in the U.S. as to other countries.

We're committed to rolling out the controls and the affirmative consent and the special controls around sensitive types of technology, like face recognition, that are required in GDPR. We're doing that around the world.

So I think it's certainly worth discussing whether we should have something similar in the U.S. But what I would like to say today is that we're going to go forward and implement that, regardless of what the regulatory outcome is.

Figure 3. Screenshot of Facebook's Congress Hearing Transcript - This screenshot is a section of Mark Zuckerberg's response to a Senator's question (Bloomberg Government, 2018)

The above figure is a screenshot of Mark Zuckerberg's statement regarding the Cambridge Analytica data leak during a Congressional hearing. Here Zuckerberg states that Facebook's privacy protection will be standardized worldwide. The critical piece in this statement is "around the world." Previously, only EU residents were given some sort of protection from data leaks; however, users who were not EU residents were left to be exploited. Facebook did not prioritize its users universally; instead, it used data protection laws to its advantage to gather user information for its business model. In this single statement by Zuckerberg, he admits that the U.S. had less strict privacy protection laws that Facebook could use to its benefit by stating, "we have somewhat different sensibilities in the U.S." The "sensibility" for protection should be consistent if Facebook values its users. Facebook saw the potential abuse in care for its users but prioritized its relationship with advertising agencies instead. While Facebook may think that it made a brave move by setting standard privacy policies worldwide, this should have been a step taken by Facebook earlier to show equal care to

its user base. Reflecting on Facebook's actions, it fails to satisfy the last stage of care, responsiveness.

Conclusion

By examining Tronto's four stages, Facebook's actions before and during the Cambridge Analytica data breach are deemed immoral through the lens of care ethics. Facebook failed to show appropriate care in each of the four stages of care. Facebook has hindered its relationship with its user base by violating the users' trust. Facebook's lack of transparency to its users resulted in a breach of trust.

Facebook has a large user base meaning that many people rely on Facebook to protect their data and provide a safe social media platform. While Facebook's main objective has always been to bring people together positively, focusing on only the good aspect of connectedness is not enough. By applying care ethics within its company's core values, Facebook will gain a broader understanding of its users' needs. This is vital information for Facebook to provide appropriate care. This lesson is not just for Facebook but for all social media platforms that collect user information and for users who choose to share their information with social media platforms.

Word Count: 3490

References

Bloomberg Government. (2018, April 10). *Transcript of Mark Zuckerberg's Senate hearing*. Retrieved from The Washington Post: https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/

Cadwalladr, C. (2018, March). *'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower.* The Guardian.

Curtis, J. (2018, March 19). Cambridge Analytica: Millions of Facebook profiles 'mined illegally'. *IT Pro*.

Data Use Policy. (2013, August 13). Retrieved from Facebook: https://web.archive.org/web/20130813123719/https://www.facebook.com/about/privacy/advertising

General Data Protection Regulation (GDPR). (2018, February 21). Retrieved from Facebook Business: https://web.archive.org/web/20180221224654/https://www.facebook.com/business/gdpr

Hopping, C., & Pro, I. T. (2018, Jul 2). Cambridge Analytica: US Congress probes data firm set up by ex-Cambridge Analytica employee. *IT Pro*.

Hu, M. (2020). Cambridge Analytica's black box. *Big Data & Society*, 1-6.

ISO/IEC 27040 (2022). Data Breach. Retrieved from SNIA: https://www.snia.org/education/online-dictionary/term/data-breach

Klaver, K., & Baart, A. (2011). Attentiveness in care: Towards a theoretical framework. *Nursing Ethics, 18(5)*, 686–693.

Kozlowska, I. (2018, April 30). *Facebook and Data Privacy in the Age of Cambridge Analytica*. Retrieved from University of Washington: https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/

Nielsen, J. (2011, September 11). *How Long Do Users Stay on Web Pages?* . Retrieved from Nielson Norman Group: https://www.nngroup.com/articles/how-long-do-users-stay-on-web-pages/

Rehman, I. u. (2019). Facebook-Cambridge Analytica data harvesting: What you need to know. *Library Philosophy and Practice*, 1-11.

Sander-Staudt, M. (2022). Care Ethics. *Internet Encyclopedia of Philosophy*, ISSN 2161-0002.

van de Poel, I., & Royakkers, L. (2011). The distribution of responsibility in engineering. In Ethics, Technology, and Engineering: An Introduction. 253–254.

Zuckerberg, M. (2018, March 21). *I want to share an update on the Cambridge Analytica situation*. Retrieved from Facebook: https://www.facebook.com/zuck/posts/10104712037900071?pnref=story