

The Questions

What responsibility should governments have?

Should governments have tighter control on firms' data collection?

If the government aggregates data, who oversees this?

In times of crisis, how is privacy ignored?

What responsibilities should corporations have?

Is it possible to constrain corporations? What punishments need to occur?

How do fines affect multi-billion dollar companies?

How clear and overt do terms & conditions need to be?

What responsibilities does the individual have?

Should users be reading the entire agreement?

How does education play into consent?

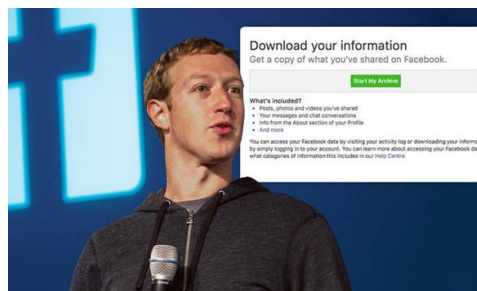
Should whistleblowers be granted protection?

Which populations are vulnerable?

Issues in Contemporary Ethics: Big Data

At a Glance

Buried inside lengthy user agreements and terms & conditions lies text that allows corporations and governments to access and use your data. This ranges from advertisements and analysis to more ethically vague purposes. Regulation exists in states, such as the Canadian Privacy Act, that limits what the government can do with your information as well as the Personal Information Protection and Electronic Documents Act (PIPEDA), which governs the private sector. However, this does not stop either from exploiting grey areas. This brief seeks to use the case study of Facebook-Cambridge Analytica scandal as a framework for the complicated issue in the digital age.



Mark Zuckerberg apologizes for the Cambridge Analytica Incident (Getty Images 2018).

Case Study: Facebook and Cambridge Analytica

In 2018, it became public that Facebook had been sharing data from “up to 87 million people” with Cambridge Analytica (CA), a political consulting and strategic communication firm. Facebook gave CA permission to make “personality tests” that they used to collect data from users. (Sanders & Patterson 2019). CA used this data to construct “personality quizzes” that grouped people and predicted sensitive personal attributes, such as their sexual orientation or religious views (Sanders & Patterson 2019). They then used this data for political ad targeting by using “shadow” ads that couldn’t be traced. As a result of the breach, Facebook faced a \$5 billion dollar fine by the American Federal Trade Commission. There was also extensive media coverage that raised public interest in privacy. While this was a large breach, data collection had been going on for over a decade at that time (Sanders & Patterson 2019). Zuckerberg had to answer to the American Congress for Facebook’s actions. While he vigorously defended his company’s decisions, he also apologized about a breach of trust. CA, on the other hand, denied wrongdoing citing that it was standard practice for the industry and legal justifications.

Implications

CA was neither the first nor the last large-scale data collection (mis)user on Facebook, with most of the collection happening on a day-to-day basis. Moreover, it is not the only company that stores information. Google, for example, uses users action and history to tailor experiences. Is this necessarily a bad thing? Imagine a YouTube homepage with irrelevant videos that you’re not interested in. This raises questions about where the line needs to be drawn between acceptable and unacceptable data collection and use.

Further Reading

O'Reilly Media

[What's Up With Big Data Ethics?](#)

Kalev Leetaru

[Is It Too Late For Big Data Ethics?](#)

Megan Ray Nichols

[Big Data Is So Large, It's Raising Privacy and Ethical Issues](#)

Julia Carrie Wong

[The Cambridge Analytica Scandal Changed the World – But It Didn't Change Facebook](#)

John Pavolotsky

[Demystifying Big Data](#)

Talia B. Gillis and Jann L. Spiess

[Big Data and Discrimination](#)

Kate Crawford

[Big Data Stalking](#)

Annika Richterich

[The Big Data Agenda: Data Ethics and Critical Data Studies](#)

Emilio Zagheni, Ingmar Weber, Krishna Gummadi

[Leveraging Facebook's Advertising Platform to Monitor Stocks of Migrants.](#)

Comparing Perspectives

In this series of Briefs, one rationalist and one alternative are explored to present contrasting views on an issue.

Contractualism

Contractualism views ethics through the lens of contracts that bind parties to a set of actions based on the values in the agreement. This would apply to terms and conditions that we accept when signing up for new accounts or being asked to access our cookies when visiting new websites. This also applies to the social contract norms of business practice with data. By accepting the terms, we are waiving a certain level of legal accountability for the site we visit. This is the defence used by groups like CA that collect data through "willing" participation and acceptance of user agreements, which provides textual legal justification. One should consider, however, what willing consent means in a contract. To fully consent, one must be able to fully understand what they are agreeing to. Some companies try to mitigate this by only allowing one to accept after they have scrolled through all the text. Perhaps Broad Laws to uphold the social contract of privacy are required. One should also consider what power companies such as Facebook have over the userbase: if everyone is online and its beneficial for business, what alternatives are available to people?

Feminist Ethics

Feminist critiques focuses on voices that are often left out of discussions regarding morality. This includes groups such as women, children, elders, and others. Elders, for example, may not have the technological background to understand rapidly changing cyber issues and can be easily scammed by preying companies, data aggregators, or scammers. On the other end, very young people sign up for social media companies due to trends, such as Tik Tok, without having the maturity needed to navigate online platforms. Of course, some companies require a certain age to use their services or planforms, but this can be bypassed by lying. On media platforms, data is never truly lost and regretful posts, images, and videos can stay in archives forever even if they're deleted publicly by users themselves; the companies own the data. This can have devastating effects for people who are reckless with their usage. Education also plays a large role in online competency. Being well-informed and knowledgeable of where your data is going is important, although it can only go so far in data protection.

Questions for Reflection

In this age, living off the grid is nigh impossible. Is it too late for big data ethics? How much bytes of data have been collected by companies like CA or Facebook that is now stored and sold beyond user control? What incentives or punishments can be effective against firms that already have so much money or power? What alternatives exist? Moreover, what purchasing power is available for data? When Facebook acquires companies like WhatsApp or Instagram, they can have access to data previously unavailable to them. Should companies be able to hand over data of users to buyers? Perhaps there should be tighter regulation or more necessary terms that companies must follow. Regardless, ethics must evolve as technology does, so that the law can as well.

Sanders, James and Dan Patterson. "[Facebook Data Privacy Scandal: A Cheat Sheet.](#)" *Tech Republic*, TechRepublic.