The power of personal data

How personal data collection and processing erodes our autonomy

Introduction

There has been a significant increase in datafication in recent years due to the widespread adoption of digital technologies and the proliferation of data-generating devices. Digital technologies, such as smartphones, wearable devices, and internet-connected devices, produce large amounts of data that can be collected and analysed for various purposes. This has led to the development of new data-driven business models, such as targeted advertising and personalized recommendations, and has also had an impact on the way that organizations and governments operate.

In this essay I will be the start of the drive for an increase in datafication and the development of the data-driven economy as well as its ethical concerns that derive from this new business model.

Furthermore, I will explain, the dangers of private date and its multiple concern to the users and Cambridge Analytica scandal and the on-going ethical concerns of private data processing and private data collection that are derived from the datafication of the new data-driven economies.

Lastly, I will be providing a few solutions such as pushing for more legislation to preserve our privacy, power and autonomy to strengthen my point of view and finish off with my own conclusion of this theme.

The start of the data-driven economy

The development of the data-driven economy has been fuelled by the proliferation of digital technologies, which have led to the collection and analysis of large amounts of data for various purposes. This data is often used to improve the efficiency and effectiveness of businesses, governments, and other organizations, and has created new opportunities for companies that are able to use data to gain insights and make informed decisions.

It all started with a company we are all familiar with, Google. After Larry Page and Sergey Brin, Google PageRank algorithm developers failed to sell Google, they required a sustainable business practice that would prevent investors from pulling out of the company, as it was not profitable (Levy, 2011, pp. 77-78).

As such Veach worked on the Google Ads platform, where he developed algorithms and tools to optimize ad targeting and placement. The theory behind optimal ad targeting was making both Google, users and advertisers happy by displaying ads that

the most relevant to the users, this way Google gets paid, the advertiser publicizes their products and the users get to enjoy a high quality search engine while only being shown ads that would peak their interest (Véliz, 2021, p.48) . A key feature of the ads platform was how it allowed Google to action the ads to the advertisers instead of the traditional purchases of a slot in a webpage of the time, now each advertiser would place bids for the displayed ads and Google would only charge them if their ads had gotten a click.

However, this revolutionised their business practices, for once the costumers were the advertisers and the users became the product of such advertisement through the collected data to be able to most optimally target us with ads. And this is how Google managed to achieve an increase in revenue from 86 million dollars in 2001 to 3,2 billion dollars in 2004, a whooping 3590% increase (SECURITIES AND EXCHANGE COMMISSION, *FORM 10-K* 2004).

As such after learning from Google incredible success and profits more companies followed

As such after learning from Google incredible success and profits many other companies followed in its footsteps and adopted similar business models thus leading to the present level of datafication in our society and live. As Google has become a pioneer in the field of digital advertising, and its advertising platform, Google Ads, has become the dominant player in the online advertising industry. Many other companies have attempted to replicate Google's success by developing their own online advertising platforms and using data-driven approaches to target and reach consumers. While Google remains a leader in the industry, there are many other companies that have also achieved significant success in online advertising, such as Facebook and Amazon.

Cambridge Analytica case study

Cambridge Analytica was a political consulting firm that used data mining and psychological profiling to influence voter opinion and behaviour. The company was accused of obtaining the personal data of millions of Facebook users without their consent, and using this data to create targeted advertising campaigns for political clients.

Cambridge Analytica obtained such data through a third-party app developed by a researcher named Aleksandr Kogan. Kogan's app, called "thisisyourdigitallife," was a personality quiz that was advertised on Facebook. When users signed up to take the quiz, they were required to grant the app access to their Facebook profile data, as well as the data of their friends.

Kogan collected this data and provided it to Cambridge Analytica, which allegedly used it to build psychological profiles of users and target them with political ads. Facebook later revealed that the data of up to 87 million users may have been improperly shared with Cambridge Analytica.

The Cambridge Analytica scandal involved a number of controversies, including:

1. Alleged misuse of personal data: Cambridge Analytica was accused of obtaining the personal data of millions of Facebook users without their consent, and using this data to create targeted advertising campaigns for political clients.
2. Alleged interference in elections: The company was accused of using its data mining and psychological profiling techniques to influence the outcome of elections, including the Brexit campaign and the 2016 U.S. presidential election (Guimón, 2018).
3. Allegations of unethical behaviour: The company was also accused of using unethical tactics, such as using fake news and disinformation to sway public opinion and target individuals designated as 'persuadable' to refrain from voting or voting for a candidate they would have otherwise not voted for (Channel 4, 2020).
4. Failure to protect personal data: The controversy raised concerns about the ability of companies to protect personal data and the potential for this data to be misused.

The outrage followed by the scandal alarmed many people that were already concerned about the potential for the misuse of personal data to impact present and future election outcomes and democracy.

The controversy also raised broader concerns about the use of data mining and psychological profiling in political campaigns, and the potential for these techniques to be used to manipulate public opinion. The scandal prompted calls for greater transparency and accountability in the use of data in political campaigns, and for stronger regulations to protect personal data and prevent its misuse.

The Cambridge Analytica scandal led to investigations by governments and regulatory bodies around the world, and prompted calls for greater protection of personal data and more stringent regulations on the use of data in political campaigns and played a role in the development and implementation of the General Data Protection Regulation (GDPR), a comprehensive data protection law that took effect in the European Union (EU) in 2018.

The GDPR introduced stronger protections for personal data and gave individuals more control over how their data is collected, used, and shared. It also established stricter rules for companies that process personal data, including requirements for obtaining consent and for protecting the data from unauthorized access or misuse.

The Cambridge Analytica scandal highlighted the need for stronger data protection measures and brought the issue of personal data privacy to the forefront of public consciousness. As a result, the GDPR was seen as a response to the concerns raised by the Cambridge Analytica controversy and similar incidents involving the misuse of personal data.

Ethical concerns and challenges to datafication

With more businesses and companies entering the data-driven economy new and more complexed algorithms were developed to process and analyse the ever increasing stream

of data that is feed to each of algorithms, however as doctor Catherine O'Neil has pointed out, all of these newly develop algorithms face incredibly challenges that are close to impossible to perfectly correct for.

An initial ethical concern from the data processing point of view is the innate discrimination that is derived from biased algorithms with toxic feedbacks. In a toxic feedback loop, the loops will be reusing incorrectly accessed information that will reinforce and amplify existing biases introduced into the algorithms during the development stage, as these biases are constantly being reinforced a biased positive stream of data is used to calculate the effectiveness of the algorithm that is used to incorrectly reinforce the strength of such flawed algorithm (O'Neil, 2018, p. 27).

Such biased results are almost impossible to question as such algorithms are often opaque, with associated scoring systems hidden from the public and worse than that from the individuals being judged from such flawed scoring methods as only the developers can see and refine how their scores were calculated. Even when are wrongly discriminated judged individuals cannot provide concrete proof of their discrimination and continuing the downward spiral of discrimination and toxicity (O'Neil, 2018, pp 7,31).

I personally believe that a system that is not completely transparent cannot be judged as impartial or unbiased as it will be impossible to be correctly accessed, tested and reviewed by not only the authority in charge but also the public domain, ensuring this way a continuity of the well-functioning of such algorithms.

Adding to these concerns on the side of the data processing of our personal data we have plenty of concerns on a much deeper level, with the very own personal data that is collected to be processed by the previously mentioned algorithms being the main target of such ethical concerns.

Of the many ethical concerns surrounding the collection and use of personal data, including the 5 most important are:

1. Privacy: The collection and use of personal data can infringe upon an individual's right to privacy, as such, the GDPR defines personal data as any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly (*Art. 4 GDPR*, 2018).
2. Autonomy: Individuals should have control over their own personal data and should be able to decide how it is used without being influenced by external forces to act disregarding our own values (Véliz, 2021, pp 106-107).
3. Collective responsibility: Personal data leaks can help facilitation violations of privacy from of other people in similar circumstances. It is also from losses of multiple individuals’ personal privacy that collective privacy is damaged and threatens national security (Véliz, 2021 pp 137-138).
4. Discrimination: The use of personal data can lead to discrimination, such as by enabling employers to exclude certain groups of people from job opportunities, refusing to provide a service of a level of service to a specific group. (Véliz, 2021 p 198).

5. Security and exploitation: The collection and storage of personal data can also raise security concerns, as data breaches can expose sensitive information to unauthorized parties. Personal data can be used to exploit individuals, such as by targeting them with misleading or manipulative advertising. (Véliz, 2021 p 198-199).

These ethical concerns highlight the need for careful consideration of the collection and use of personal data, as well as the need for strong data protection regulations to safeguard individuals' privacy and autonomy.

The toxicity of data

Our personal data has been considered toxic for us as individuals, companies and societies.

Individuals because it is incredibly personal and sensitive, containing our hidden desires, fear and secrets and can lead to identity theft, financial loss, and damage to their reputation. It can also erode trust and create a sense of vulnerability, as people may feel that their personal information is not being properly protected.

Companies because it is virtually impossible to always protect and defend it from attackers. And the loss or exposure of data can also be financially costly, as it can lead to legal penalties, financial fines, and damage to the company's reputation. It can also lead to the loss of customer trust and loyalty, as people may be less likely to do business with a company that they feel is not protecting their personal information (Schneier, 2016).

This is why in this essay I wanted to analyse the most prominent case of mishandled usage of personal data in the last decade, Cambridge Analytica scandal to properly exemplify the dangers and how the toxicity of personal data have far-reaching consequences on society and individuals.

One major risk is the potential for data misuse, such as when companies or governments collect and analyse personal data in ways that infringe on individuals' privacy. This can lead to the erosion of personal autonomy and freedom, as people may feel that their actions and decisions are being monitored and influenced by external parties (Schneier, 2016).

Another danger of toxic data is the potential for it to be used to spread misinformation or propaganda, which can have serious consequences for public discourse and decision-making. In some cases, toxic data can be used to manipulate or polarize public opinion, leading to social unrest and conflict.

Finally, the mismanagement or mishandling of data can also lead to security breaches, where sensitive or personal information is exposed or stolen. This can have grave consequences for individuals, including identity theft and financial loss.

Solutions

It is true that many laws and social norms that are widely accepted today were once highly controversial and met with significant resistance, that is why to protect our privacy landscape we must first persuade the others to protect their own and our shared and collective privacy.

One way to persuade others to protect their own and our privacy is to educate them about the importance of privacy and the potential risks of sharing personal information online. It is also important to advocate for stronger privacy laws and regulations, and to support companies and organizations that prioritize privacy.

Another way to protect our privacy is to use tools and practices that safeguard personal information, such as using a virtual private network (VPN) when connected to the internet, using strong and unique passwords for online accounts, being cautious about sharing personal information online, therefore also protecting others as a collateral of our protection.

Participating in grassroots campaigns is a powerful way for individuals to advocate for stronger privacy laws and protections. Grassroots campaigns involve individuals coming together to raise awareness about an issue and to advocate for change.

Donating to privacy-focused organizations is a great way to support the efforts of these organizations and to advocate for stronger privacy laws.

By raising awareness about privacy issues and the potential risks of sharing personal information online, individuals can help to build support for stronger privacy laws and protections.

Using our consumer power we may choose to support businesses and organizations that prioritize privacy and consider the privacy practices of the companies you do business with. When you choose to do business with companies that prioritize privacy, you are helping to create a market demand for privacy-protective products and services. This, in turn, can incentivize other companies to adopt stronger privacy practices in order to remain competitive.

By taking action and advocating for stronger privacy laws, individuals and organizations can help to create a more privacy-protective society.

Conclusion

It is true that not everyone values privacy in the same way, and that some people may be willing to sacrifice more of their privacy for convenience or other benefits. However, it is important to recognize that even if an individual is not concerned about their own privacy, they may still be affected by the lack of privacy of others. For example, if a person's personal information is exposed online, it can lead to identity theft or other financial or personal harms. Additionally, the loss of privacy can have broader societal consequences, such as the erosion of civil liberties and the abuse of power. As such, it is

important for individuals to consider not only their own privacy, but also the privacy of others and the impact on society as a whole when making decisions about how much privacy to sacrifice.

All of the measures can make a difference and save you from violations of your own privacy but no method will ever guarantee privacy so it must be up to ourselves to decide how much our privacy worth and plan accordingly to protect it, its future and act accordingly, constantly defending it against the constant lobbying of the tech giants who do not have our best interest in mind (Shaban, 2021).

Bibliography:

Levy, S. (2011) "Googlenomics: cracking the code on internet profits," in *In the plex how google thinks, works, and shapes our lives*. New York: Copyright © 2011 by Steven LevyReprinted by permission of Simon & Schuster, Inc, pp. 77–78.

Véliz (2021) "How did we get here?," in *Privacy is power: Why and how you should take back control of your data*. Brooklyn: Melville House, p. 48.

(2004) *FORM 10-K* . Washington, D.C. 20549 (Commission file number: 000-50726). Available at: https://www.sec.gov/Archives/edgar/data/1288776/000119312505065298/d10k.htm (Accessed: January 5, 2023).

O'Neil, C. (2018) "Shell shocked: My journey of disillusionment," in *Weapons of math destruction how big data increases inequality and threatens democracy*. London: Penguin Books, p. 27.

O'Neil, C. (2018) "Bomb parts: what is a model," in *Weapons of math destruction how big data increases inequality and threatens democracy*. London: Penguin Books, pp. 7,31.

Channel 4 Team, C.4 N.I. (2020) *Revealed: Trump campaign strategy to deter millions of black Americans from voting in 2016, Channel 4 News*. Job Rabkin, Guy Basnett, Ed Howker, Janet Eastham and Heidi Pett. Available at: https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016 (Accessed: January 6, 2023).

Guimón, P. (2018) *"Brexit wouldn't have happened without Cambridge Analytica", EL PAÍS English Edition*. El País. Available at: https://english.elpais.com/elpais/2018/03/27/inenglish/1522142310_757589.html (Accessed: January 6, 2023).

Art. 4 GDPR – definitions (2018) *General Data Protection Regulation (GDPR)*. Available at: https://gdpr-info.eu/art-4-gdpr/ (Accessed: January 8, 2023).

Véliz (2021) "Privacy is power," in *Privacy is power: Why and how you should take back control of your data*. Brooklyn: Melville House, pp. 106–107.

Véliz (2021) “Toxic data,” in *Privacy is power: Why and how you should take back control of your data*. Brooklyn: Melville House, pp. 137–138.

Véliz (2021) “Pulling the plug,” in *Privacy is power: Why and how you should take back control of your data*. Brooklyn: Melville House, p. 198.

Véliz (2021) “Pulling the plug,” in *Privacy is power: Why and how you should take back control of your data*. Brooklyn: Melville House, pp. 198-199.

Schneier, B. (2016) *Data Is a Toxic Asset, So Why Not Throw It Out?*, *Schneier on security*. CNN. Available at: https://www.schneier.com/essays/archives/2016/03/data_is_a_toxic_asse.html (Accessed: January 9, 2023).

Schneier, B. (2016) *Data Is a Toxic Asset, So Why Not Throw It Out?*, *Schneier on security*. CNN. Available at: https://www.schneier.com/essays/archives/2016/03/data_is_a_toxic_asse.html (Accessed: January 9, 2023).

Shaban, H. (2021) *Google for the first time outspent every other company to influence Washington in 2017*, *The Washington Post*. WP Company. Available at: https://www.washingtonpost.com/news/the-switch/wp/2018/01/23/google-outspent-every-other-company-on-federal-lobbying-in-2017/ (Accessed: January 9, 2023).