Libera Università Internazionale degli Studi Sociali Guido Carli

DEPARTMENT OF ECONOMICS AND FINANCE

Bachelor's Degree in Economics and Business

Chair of IO and Competition Theory

"The Threat of Data: an analysis of social media industry and privacy concerns"

SUPERVISOR

Prof. Gian Luigi Albano

CANDIDATE

Simone Soldato (253881)

Academic Year 2022/2023

If you place your head in a lion's mouth,
then you cannot complain if one day it bites it off.

Agatha Christie, Novelist.

TABLE OF CONTENTS

INTRODUCTION

Every morning a teenager wakes up, takes out his phone, opens Instagram and takes a peek at his feed. Then he opens WhatsApp or iMessage and replies to texts from friends who in an hour's time he will see live at school. Meanwhile, at a major international airport a businesswoman wrote a LinkedIn post with her latest business success and tweeted to complain about the delay of her plane. And again, a gentleman posted a souvenir photo of his last vacation on Facebook with the hashtag #TBT as he was about to break away from his exhausting night shift.

It is a fact that social networks have now become an integral part of our lives. They come to our rescue in moments of boredom, they help us when we need news or information, and they keep alive relationships that perhaps because of the distance would be lost. They have become the glue of our society during the pandemic and one of the main causes of any harm of this century. All this at no cost, or almost. The real currency of this industry is our data; this is a fact that many are aware of by now, but how this data is then managed and what are the tools at our disposal to protect ourselves remains a placid mystery for most of users. We could therefore rejoin the theory of the two-sided platforms in which there is a side that has the impression of not paying, but in reality, is paying by giving access, free of charge, to its data. An implicit price which, in most cases, is difficult for users to identify. The final intent of this thesis is precisely to analyze the social media market and its contradictions, starting from the Cambridge Analytica case study, highlighting the peculiar elements of this industry and the main regulations in terms of personal data management and then reporting, finally, how these are only partially adopted by companies to encourage the registration of the greatest possible number of users.

1. CAMBRIDGE ANALYTICA SCANDAL

On March 18, 2018, The New York Times[1] and the Guardian[2] published a series of articles reporting the incorrect use of a huge amount of data collected through Facebook by a British consulting firm, Cambridge Analytica. The accusation was that the data of the American users of the main Meta platform were exploited, without their consent of course, in profiling operations aimed at benefiting the electoral campaign of the forty-fifth president of the United States, Donald Trump.

1.1 THE FOUNDATION

Cambridge Analytica was founded in 2013 as a division of the private intelligence firm SCL Group, which operated in the military and political spheres of British society. The company proposes itself as leader of behavioral analysis and profiling activities for marketing purposes. The idea was to use the new theories of micro-targeting, which saw the fusion of data analysis with the key concepts of psychometrics, to profile users.

When we talk about micro-targeting (known more as micro-marketing) we are essentially referring to the application of geodemographic characteristics to the main precepts of consumer marketing with the intention of promoting a consumer experience that is customized and that fully reflects his needs. In 1994, Kotler defined micromarketing as "a type of target marketing in which companies tailor their marketing programs (products, advertising, sales promotions, and personal selling efforts) to the needs and desires of narrowly defined geographic, demographic, socioeconomic, psychographic, or benefit segments."[3]

However, it is clear how this form of hyper-segmentation can only rely on the availability of data. The more data companies have available, the easier it will be to create a product or service that is in line with what the consumers are looking for. Applying these concepts to a political context, theoretical studies suggest that the choice of vote of a rational individual can be associated with a real choice of consumption. Since the individual is assumed as rational, this will vote only when the

[1] Matthew Rosenberg, Sheera Frenkel, "Facebook's role in Data Misuse Sets Off Storms on Two Continents", The New York Times. (March 18, 2018) https://www.nytimes.com/2018/03/18/us/cambridge-analytica-facebook-privacy-data.html

[2] Carole Cadwalladr, "I made Steve Bannon's psychological warfare tool: meet the data war whistleblower", Guardian (March 18, 2018) https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

[3] Kotler, P. (1989), "From mass marketing to mass customization", Planning Review, SeptemberOctober, pp. 10-23 and 47.

expected benefits exceed the expected costs related to a vote. It is the so-called *Paradox of Voting*[4], a theory that was born back in 1793 by Nicolas De Condorcet.

When the cost of voting is virtually zero, the benefits outweigh the costs, and the individual will go to vote. Alexander Nix, the founder of Cambridge Analytica, decided to incorporate these concepts in his company's strategy which was precisely a micro-targeting one aimed at minimizing the individual costs of a vote through subliminal messages of advertising nature on the social profiles of the "swing voters"; those who can represent the turning point in an election.

One of the implicit costs of an electoral round is precisely that deriving from the cost related to getting informed, which is a necessary step to be able to cast one's vote. If citizens are unaware of electoral agendas, what candidates say, or who the candidates are, they will never have the tools to get to the polls. However, this duty is, in a way, the most "boring" part of the whole process. Following the talks, reading the newspapers, or listening to the radio services takes time away from other activities and, going back to the discussion above, if a citizen is rational and the utility deriving from political participation is very low, he will prefer to devote himself to something else rather than following the electoral campaign. Social networks simplified this process and today these are the fastest and cheapest tool in terms of cost and time to be able to get information. The Pew Research Center, a prominent American statistical Institute, conducted research on how American citizens consume news[5], reporting how they feel more informed thanks to the web. Going into detail, 75% of the American population would feel better informed about national affairs thanks to the use of the internet, while 72% of digital users believe that the internet has allowed them to express ideas and thoughts more easily (Fig.1). If we then analyze the political issue, 2020 research[6], also by the Pew Research Center, reported that 44% of young people between 18 and 29 years old get information on the political

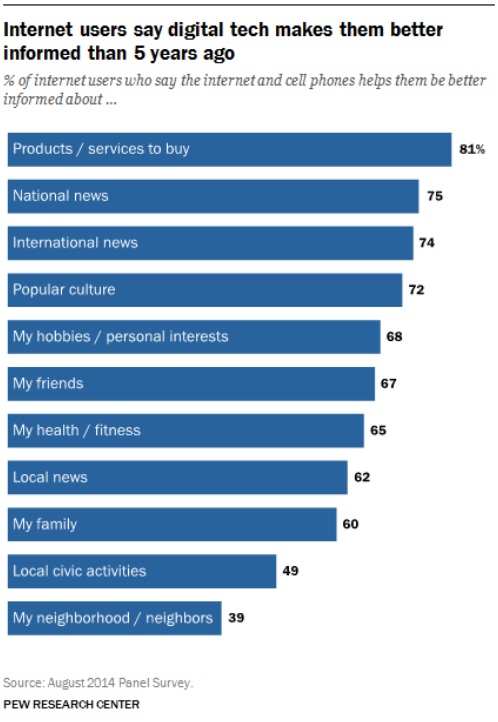


Figure 1

[4] Wikimedia Foundation (2022, December 9). *Paradox of Voting*. Wikipedia. Retrieved February 15, 2022 from https://en.wikipedia.org/wiki/Paradox_of_voting

[5] Kristen Purcell, Lee Rainie (2014, December 8). Americans feel better informed thanks to the internet. Pew Research Center. Retrieved February 15, 2022 from https://www.pewresearch.org/internet/2014/12/08/better-informed/

[6] Amy Mitchell, Mark Jurkowitz, J. Baxter Oliphant, Elisa Shearer (2020, July 30). Demographics of Americans who get most of their political news from social media. Pew Research Center. Retrieved February 15, 2022 from https://www.pewresearch.org/journalism/2020/07/30/demographics-of-americans-who-get-most-of-their-political-news-from-social-media/

situation mainly through social media with not very different statistics in the groups with similar demographic features (Fig.2).

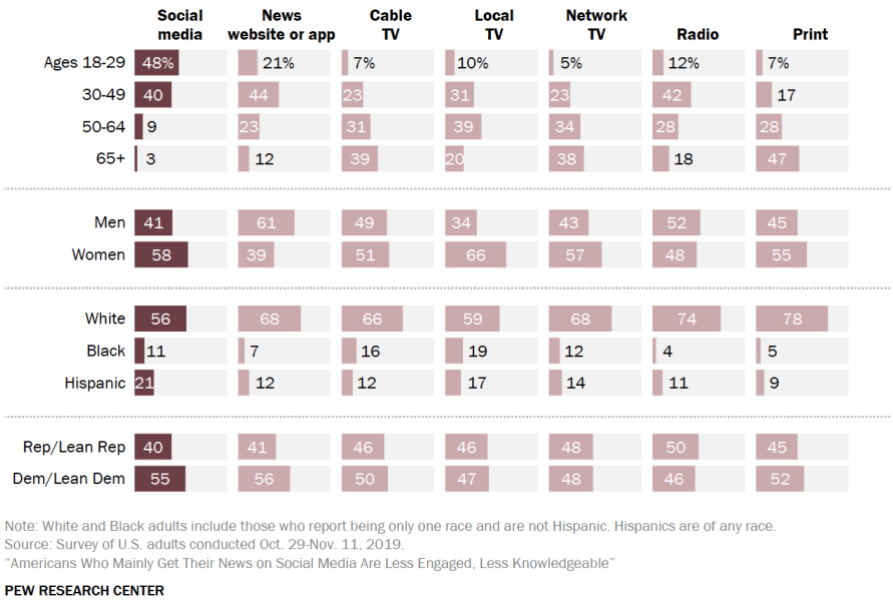
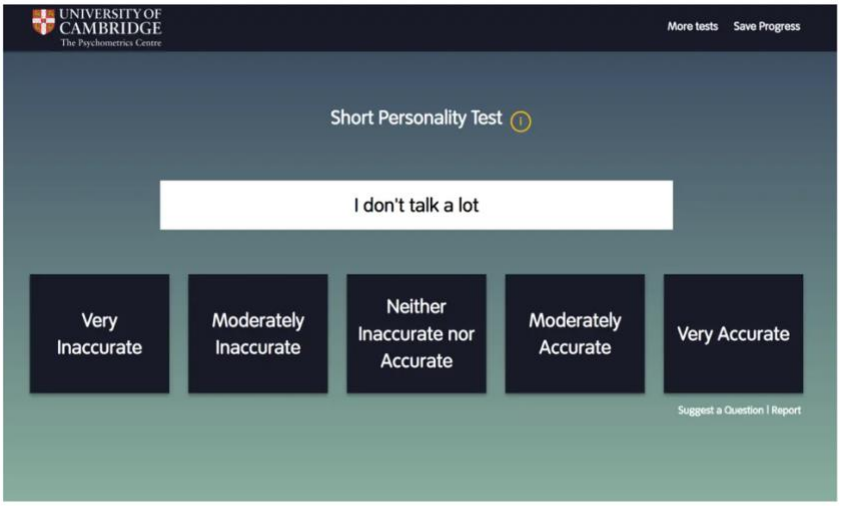


Figure 2

This means that reaching these segments of the population on social media could be a fairly effective method of transferring a candidate's message and facilitating adherence to one political party over another, which Cambridge Analytica actually did.

In 2014, all the regular American users of Facebook will have come across a test like this one (Fig.3) reconstructed by the University of Cambridge [7] following the scandal that struck Cambridge Analytica a year later.



University of Cambridge

Figure 3

[7] A sample of the test can be found at this website (University of Cambridge): https://discovermyprofile.com/tests

Tests of this type are defined as "Big Five personality traits test" or "OCEAN test" and they are used to favor grouping of individuals based on their personal characteristics. When applied to personality questionnaire responses, factor analysis[8] tests linguistic associations: some words used to describe aspects of personality are commonly applied to the same person. For instance, someone described as “conscientious” is more likely to be referred to as "often prepared" rather than "messy". These associations point to five broad dimensions which are frequently used to characterize human personality, temperament, and psyche. Although this model was born in 1958 by two psychologists, Ernest Tupes and Raymond Christal, in reality it did not find great success until the 90s[9] of the last century.

In 2009 Arthur Poropat in his *A Meta Analysis of the Five-Factors Model of Personality and Academic Performance*[10] suggested that this test could be used to analyze the correlation between students' academic performance and their personality. Over time, the 5 most common and prevailing personality traits in our society have been defined: Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism which together make up the acronym OCEAN from which the test takes its name.

Each of these traits was then split in two to highlight how even within the same psychological trait there were two distinct still correlated currents that identify the level of personality within the main domain. For instance, consider an individual whose character falls within the domain of extraversion. This person will display an open, jovial demeanor and be prone to interacting with others. However, this interaction can take on two different facets: on the one hand, extroversion could lead to generalized enthusiasm, or on the other hand to assertiveness related to a particular situation that pushes the individual to experiment and satisfy the typical curiosity of his domain.

Below, a brief explanation for each psychological trait and the sentences that would correspond to it within the OCEAN test.

[8] Factor analysis is a statistical method used to reduce a large number of variables into fewer numbers of factors.
[9] Goldberg, L.R. (1993). The structure of phenotypic personality traits. American Psychologist, 48(1), 26–34. https://doi.org/10.1037/0003-066x.48.1.26
[10] Poropat, A. E. (2009). A meta-analysis of the five-factor model of personality and academic performance. Psychological Bulletin, 135(2), 322–338. https://doi.org/10.1037/a0014996

- **Openness to experience**

  Mainly related to a general appreciation for art, emotion, unusual ideas, imagination, curiosity, and diversity of experience. People who are willing to try new things are open and curious, emotionally aware, visually sensitive, and adventurous. Especially in comparison to closed people, they are more imaginative and conscious of their emotions. High openness can be interpreted as unpredictability, or a lack of concentration and it makes people more likely to engage in dangerous behaviors or drug use. Furthermore, people with high openness are said to seek self-actualization specifically through intense, euphoric experiences. Those with low openness, on the other hand, seek fulfillment through perseverance and are described as pragmatic and data driven.

  Referring sentences: I have a rich vocabulary; I have a vivid imagination; I have excellent ideas.

- **Consciousness**

  Conscientiousness is the character trait of being extremely cautious or meticulous. It entails a desire to accomplish a task well and to take an individual's duties to others seriously. These people are efficient and organized, and they tend to be self-disciplined, act dutifully, and strive for success; they prefer to schedule rather than act impulsively; and they are generally dependable.

  Referring sentences: I am always prepared; I pay attention to details; I get chores done right away.

- **Extraversion**

  Extraversion is the tendency to seek gratification from sources other than oneself. Extraverts are enthusiastic, talkative, assertive, and gregarious, and they genuinely love human interactions since they feel energized by the presence of other people. They enjoy activities involving massive social groups, such as parties, community activities, public demonstrations, and business or political organizations. They also perform well in groups. Time spent alone is less rewarding for an extroverted person than time spent with others.

  Referring sentences: I am the life of the party; I feel comfortable around people; I start conversations.

- **Agreeableness**

  Individual differences in the overall interest for social harmony are reflected in the agreeableness characteristic. Those who are agreeable value getting along with others. They are typically regarded as helpful, trusting, giving, kind, and eager to put others' needs ahead of their own and tend to have a positive outlook on people.

  Disagreeable people prioritize their own needs over those of others. They generally don't care about other people's welfare and are less likely to sacrifice themselves for others.

  Referring sentences: I am interested in people; I sympathize with others' feelings; I have a soft heart.

- **Neuroticism**

  Those who score highly on the neuroticism scale are more prone than the average person to be moody and to feel emotions like worry, anxiety, wrath, frustration, jealousy, and melancholy. Such individuals are supposed to react more negatively to pressures and to regard commonplace events, including mild frustrations, as being impossibly challenging.

  According to research, those who score highly on the neuroticism scale are more likely to have the types of symptoms commonly referred to as "neuroses" and common mental diseases.

  Referring sentences: I get stressed out easily; I worry about things; I am easily disturbed.

Whenever a user decided to undergo this type of test (very often used and presented as an innocent game to most Facebook users), Cambridge Analytica obtained information relating to his personal characteristics and, thanks to an initial disclaimer that had to be accepted before playing, also personal information published on Facebook, page likes, current city, and the location in real-time.

All information that once combined provided the voter's identikit and facilitated the work of Cambridge Analytica that would start exposing the user with ads and trying to influence his choice of the vote against a party or a particular candidate as shown in the next paragraph.

1.2 DATA MISUSE

- **Ted Cruz Electoral Campaign**

A few months before the American presidential elections of 2016, the primaries were held between the two American parties, the Republicans and the Democrats. In the Democratic Party there was a challenge between Bernie Sanders and Hillary Clinton leading to a victory with 55% of the votes of the latter. In the Republican Party, on the other hand, the clash was a little more articulated. After the ascension of Obama, who had routed his suitors both in 2008 and 2012, the conservative party was having great difficulty staying on its feet, due to an uncertain political agenda and a series of schisms that struck it during Obama's presidency, which saw a collapse in the popularity of its exponents. The challenge, therefore, was not only to reach the White House but to reform the party and bring it back to the glory of the Bush family.

Two were the main protagonists of this clash: Donald Trump and Ted Cruz. The latter had been a federal senator from Texas since 2013, a red state, and in 2016 he had decided to compete against Trump in the party primaries. To manage his political campaign, he had decided to hire Cambridge Analytica which, it will be reported later, would have been paid 5.8 million dollars in services related to targeting of American republican citizens entitled to vote to whom personalized advs were submitted to channel their vote towards Ted Cruz. The latter, once the scandal came out, allegedly stated that: "Cambridge Analytica was an outside vendor that the campaign hired to assist in data analysis and online advertising, and they worked for the campaign, pursuant to the contract. Cambridge Analytica represented to the campaign that all data in their possession were legally obtained and that they were in compliance with all applicable laws and regulations, and the campaign relied on those representations"[11]. However, no accusation or judicial measure will be moved on this occasion. Nonetheless, Ted Cruz's electoral campaign marks the first episode in which Cambridge Analytica will find itself entangled with illegal actions in the field of personal data processing, but above all, on this occasion, the top management of the company could have come into contact with Donald J. Trump.

[11] Samsel, Hamp; Svitek, P. (2018, March 20). Ted Cruz says Cambridge Analytica told his presidential campaign its data use was legal. The Texas Tribune. Retrieved February 18, 2023, from https://www.texastribune.org/2018/03/20/ted-cruz-campaign-cambridge-analytica/

- **Donald Trump 2016 Presidential campaign**

After winning the party primary, Trump found himself challenging Hillary Clinton for the role of President.

Mrs. Clinton was a tough opponent for Trump. She was well-liked by much of the American population, appreciated for her acumen and her sense of duty, admired for the resilience with which she had held court during the presidency of her husband, Bill Clinton, and her calm reaction, worthy of a figure institutional, in the face of the Lewinski scandal[12].

In Fig.4[13] it is possible to see a demographic profile of Trump and Clinton's supporters.

Trump hired Cambridge Analytica to run his campaign, and the firm began providing a similar set of services as Cruz's campaign, analyzed earlier. The idea was to use social media to favor a polarization of public opinion[14]. As a consequence, the faithful supporters of the Republican party were delivered a series of ads that saw Trump as the new President and all the information necessary to vote correctly. All the swing voters, for their part, were instead subjected to a smear campaign against the Democratic candidate.

In fig.5[15] it is provided an example of how ads would look like.

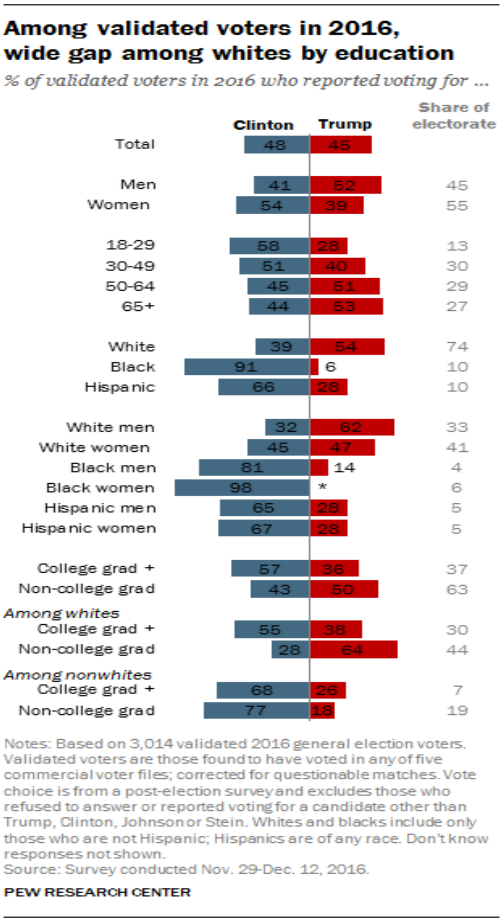


Figure 4

[12] The Clinton-Lewinski scandal was a sex scandal involving Bill Clinton, President of the United States, and Monica Lewinski, a White House intern. For reference, *see*: Posner, R.A. (2000). An affair of state the investigation, impeachment, and trial of President Clinton. Harvard University Press.

[13] Jones, B. (2022, October 26). An examination of the 2016 electorate, based on validated voters. Pew Research Center - U.S. Politics & Policy. Retrieved February 19, 2023, from https://www.pewresearch.org/politics/2018/08/09/an-examination-of-the-2016-electorate-based-on-validated-voters/

[14] Political polarization is becoming a huge problem in the United States leading to xenophobia, social disorders, and social segmentation. There is now a huge debate on whether the bipartisan system adopted by the United States is still a good choice for the American political system. For reference, *see*: Geiger, A. (2021, April 9). Political polarization in the American public. Pew Research Center - US Politics & Politics. Retrieved February 19, 2023 from https://www.pewresearch.org/politics/2014/06/12/political-polarization-in-the-american-public/

[15] Lewis, P., & Hilder, P. (2018, March 23). Leaked: Cambridge Analytica's blueprint for trump victory. The Guardian. Retrieved February 19, 2023, from https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analytics-blueprint-for-trump-victory

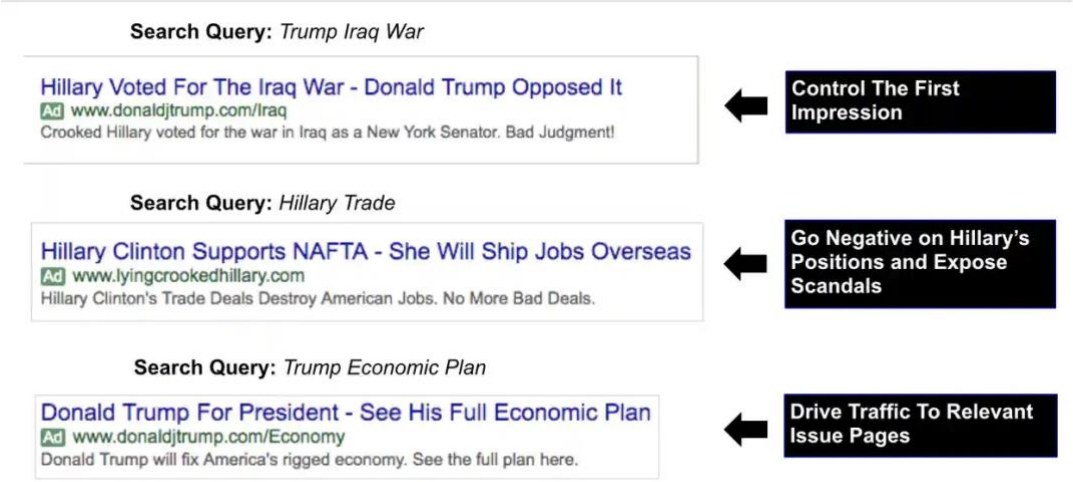


Figure 5

Hillary Clinton was pampered as incapable of running a nation and accused of corruption during her husband's presidency. All allegations that found no foundation of any kind or that, at least, could not be verified, but which in one way or another managed to breach the psyche of the uncertain. The turning point, which decreed the decisive sinking of the candidate, was at the end of the presidential campaign. A few weeks before the Americans went to the polls, Hillary Clinton fell ill which was filmed and broadcast by major news outlets. Clinton had pneumonia[16], which was treated in time for the electoral runoff. But even if she reassured her voters about her state of health as highlighted in fig. 6[17], this small inconvenience decreed a series of ads in favor of Trump which partially shifted the favor of public opinion.

[16] BBC. (2016, September 13). Hillary Clinton 'kept pneumonia diagnosis from most of team'. BBC News. Retrieved February 19, 2023, from https://www.bbc.com/news/election-us-2016-37346293
[17] Clinton, H. (2016, September 12). Thanks to everyone who's reached out with well wishes! I'm feeling fine and getting better. -H. Twitter. Retrieved February 19, 2023, from https://twitter.com/HillaryClinton/status/775435555601543168

Figure 6

If during the polls Clinton was given as the certain winner of this political confrontation[18] with a significant difference from her rival, there will be just over two percentage points separating them which, added to the preference of the Big Voters, will lead to Clinton's defeat.

On 23 March 2018, a few days after the publication of the first article accusing Cambridge Analytica of having improperly exploited the personal data of millions of users, the Guardian published another article saying there would have been interference by the company in the electoral campaign and as proof of this some private internal documents were passed on to the press. Subsequently, the Guardian decided to interview[19] Brittany Kaiser, director of Cambridge Analytica who had left the company just over two weeks earlier due to an unresolved contract dispute. Kaiser allegedly provided the British newspaper with a 27-page confidential document explaining in detail all the strategies adopted during Trump's electoral campaign. Kaiser says she did not actively work on the campaign, however as a director she had access to these documents which were used by the company as an information leaflet for future customers once a non-disclosure agreement was signed. Kaiser says that initially there was no plan to use Facebook users' data, but only those produced and provided by the Republican party which, however, presented some problems as she later explained to the Guardian: "There was no database of records. There were many disparate data sources that were not connected, matched or hygiened. There was no data science programme, so they weren't undertaking any modelling. There was no digital marketing team"[20]. The leaked document suggests in a page how Cambridge Analytica was able to monitor the effectiveness of the messages produced on the different types of votes by analyzing the levels of engagement on social platforms including Facebook, Twitter, and Snapchat.

[18] Wikimedia Foundation. (2022, December 30). Nationwide opinion polling for the 2016 United States presidential election. Wikipedia. Retrieved February 19, 2023, from https://en.wikipedia.org/wiki/Nationwide_opinion_polling_for_the_2016_United_States_presidential_election
[19] *Id. supra note 15.*
[20] *Id. supra note 15.*

One of the more successful advertisements, in Kaiser's opinion, was a native advertisement[21] on the political news website Politico[22], which was also highlighted in the presentation. For several weeks, visitors from a list of important swing states saw an interactive graphic that appeared to be a piece of journalism and purported to contain *10 embarrassing truths about the Clinton Foundation*. Kaiser says it was created by Politico staff[23] and it was reported in the 27-page Cambridge Analytica presentation as a huge success since it created a level of engagement of almost four minutes. According to the presentation, Cambridge Analytica and Trump campaign adopted another innovative technique allowing people to boost viral tweets with a set of pre-determined hashtags.
Kaiser recounts how similar strategies were employed during the political campaign for the UK's EU membership.

- **Brexit**

On 31 January 2020, The UK officially leaves the European Union. The months preceding that decision had seen a strong and tight campaign for abandonment, called LEAVE.EU[24], wanted by the UK Independence Party[25]. The latter was founded shortly after the sovereign debt crisis[26] of 2010, following which a growing anti-European sentiment had spread in The United Kingdom.
Great Britain had efficiently withstood the crisis that the European Union had gone through and was particularly upset when the Union used some of the common funds[27] to help other member states that found themselves in serious economic difficulties such as Italy, Cyprus, and Greece. It was in this climate that the UK Independence Party took hold, but remained silent until 2015, the year in which the possibility of leaving Europe began to make its way into the political debate. LEAVE.EU was the natural evolution of this popular sentiment. There was a need to campaign for the referendum, so some of the major financiers of the UK Independence party decided to shift part of their capital

[21] Sponsor-generated content: Ten inconvenient truths about the Clinton Foundation. (n.d.). Retrieved February 19, 2023, from https://www.politico.com/sponsor-content/2016/08/inconvenient-truths-about-clinton-foundation
[22] Politico is an American newspaper specialized in political news information worldwide. For reference, see: www.politico.com
[23] Politico will defend himself by saying that an information banner on the content created by the sponsor had been placed to protect users and that no newspaper columnist had collaborated in the creation of that specific content. However, one still wonders how it is possible that such an authoritative newspaper has not analyzed the piece before authorizing its publication.
[24] LEAVE.EU website is not in service anymore. However, from internet archives it is possible to find a reconstruction of what it looks like. For reference, see: TheKnow - our campaign. Our Campaign - Leave.eu. (n.d.). Retrieved February 19, 2023, from https://web.archive.org/web/20151013010834/http://leave.eu/en/our-campaign
[25] The UK Independence Party is a Eurosceptic, right-wing party active from 2010s and now led by Neil Hamilton.
[26] For reference, *see*: Kenton, W. (2022, December 24). European sovereign debt crisis: Eurozone crisis causes, impacts. Investopedia. Retrieved February 19, 2023, from https://www.investopedia.com/terms/e/european-sovereign-debt-crisis.asp
[27] For reference, *see*: European Council. (2011). (rep.). Draft European Council decision . Retrieved February 19, 2023, from https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/118578.pdf#page=6.

towards this campaign which officially became that of the conservative wing. To handle it all, Cambridge Analytica was hired. In the referendum of July 2016, *leave* won with 51.89% of the valid votes[28]. David Cameron, Prime Minister at the time, who had already rejected the idea of instituting a referendum to leave Europe in 2012, resigned and Theresa May took his place. Before Brexit, Prime Minister David Cameron told the World Economic Forum in London that Russia "would be happy"[29] with a positive outcome of the referendum. Boris Johnson characterized these statements as "a bit much"[30] and definitely not fitting the role of a Prime Minister. But in January 2018, the United States Senate released a minority report entitled *Putin's Asymmetric Assault On Democracy In Russia And Europe: Implications For U.S. National Security*[31] affirming that the US government entered in possession of information according to which Putin's government interfered with the British democratic referendum by favoring the vote towards *leave* through cyber hacking, disinformation and corruption. A few months later, in June 2018, the Guardian published an article[32] suggesting that Arron Banks, one of of the main financiaries of the UK Independence Party and LEAVE.EU, received the offer of a Russian gold mine and held various private meetings with the Russian ambassador in London. Summoned before the Parliamentary Commission set up to investigate the incident, Banks admitted that he did indeed lie about his relations with the Russians but refused to answer any further questions about it. The established parliamentary committee continued its work and in July published a document[33] in which it effectively acknowledged that Russia had interfered with the normal democratic process through an "unconventional warfare"[34] via Twitter and other media targeting British citizens. However, Arron Banks was not only the main benefactor of LEAVE.EU, or the one who had contacts with the Russians, he was also the one who hired Cambridge Analytica to manage the Conservative campaign during the referendum. Brittany Kaiser, the whistleblower who provided the 27-page document on Cambridge Analytica's handling of the Trump campaign, claimed that the datasets exploited by LEAVE.EU were provided by Cambridge Analytica[35].

---

[28] For reference, *see*: BBC. (n.d.). EU referendum results. BBC News. Retrieved February 19, 2023, from https://www.bbc.co.uk/news/politics/eu_referendum/results

[29] MirrorPolitics. (2016, May 17). David Cameron just claimed ISIS supports the EU referendum 'leave' campaign. mirror. Retrieved February 19, 2023, from https://www.mirror.co.uk/news/uk-news/isis-backs-brexit-david-cameron-7988647

[30] *Id.*

[31] U.S. Senate. (2018). (rep.). Putin's Asymmetric Assault On Democracy In Russia And Europe: Implications For U.S. National Security. Retrieved February 19, 2023, from https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

[32] Cadwalladr, C., & Jukes, P. (2018, June 16). leave. EU faces new questions over contacts with Russia. The Guardian. Retrieved February 19, 2023, from https://www.theguardian.com/uk-news/2018/jun/16/leave-eu-russia-arron-banks-andy-wigmore

[33] Disinformation and 'fake news': Interim report - digital, culture ... (n.d.). Retrieved February 19, 2023, from https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36308.htm

[34] *Id.*

[35] Weaver, M. (2018, April 17). Cambridge Analytica: Ex-director says firm pitched detailed strategy to leave.EU. The Guardian. Retrieved February 19, 2023, from https://www.theguardian.com/uk-news/2018/apr/17/cambridge-analytica-brittany-kaiser-leave-eu-brexit

As a result, Arron Banks has been investigated by the British National Crime Agency[36], while Cambridge Analytica was immediately cleared of all charges once the UK Information Commission found no data to support a regulatory intervention by the public authority.

1.3 RESPONSES AND REACTIONS

- **Facebook**

Shortly after the scandal, Facebook CEO Mark Zuckerberg gave a video interview to CNN[37] in which he defined everything that happened as "a major breach of trust". In American Corporate Law, a *breach of trust* is defined as "the conduct of a trustee appointed under a trust and their failure to discharge their duties as stipulated by the trust instrument and general duties under the law"[38]. A trustee primarily has a fiduciary relationship with the beneficiary and if he were to be involved in a breach of trust in a situation where he would put his own interests above those of the beneficiary, he could be charged with a breach of the duty of loyalty[39]. What happened between Facebook and Cambridge Analytica is a similar case since Cambridge Analytica allegedly put its interests above those of Facebook by exploiting user data for purely personal and selfish interests.

One of the very first actions that Zuckerberg admitted he took to safeguard users' personal data is to restrict developers' access to information so that they cannot develop narcissistic interests.

“One is making sure that developers like Aleksandr Kogan[40], who got access to a lot of information and then improperly used it, just don't get access to as much information going forward. So we are doing a set of things to restrict the amount of access that developers can get going forward”[41]. Continuing the interview, he added: "But the other is we need to make sure that there aren't any other Cambridge Analytics out there. Right, or folks who have improperly accessed data. So, we're gonna go now and investigate every app that has access to a large amount of information from before we locked down our platform. And if we detect any suspicious activity, we're gonna do a full forensic audit"[42]. However, there is no information about how this forensic was carried out nor if it was actually carried out by a private company outside Meta, which did not reassure the plethora of

[36] Investigation into payments made to better for the country and leave.EU. Electoral Commission. (n.d.). Retrieved February 19, 2023, from https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/our-enforcement-work/investigations/investigation-payments-made-better-country -and-leaveeu

[37] Segall, L. (2018, March 21). CNN interview: Read Mark Zuckerberg's remarks. CNNMoney. Retrieved February 20, 2023, from https://money.cnn.com/2018/03/21/technology/mark-zuckerberg-cnn-interview-transcript/index.html

[38] Breach of trust - law definition • sewell & kettle lawyers. Sewell & Kettle Lawyers. (2022, January 31). Retrieved February 20, 2023, from https://sklaw.au/dictionary/breach-of-trust/

[39] For reference, *see*: Bainbridge, S.M. (2020). Corporate Law. Foundation Press.

[40] Aleksandr Kogan is known for having developed the app that allowed Cambridge Analytica to collect personal details of 80 million users.

[41] *Id.* supra note 37.

[42] *Id supra note* 37.

investors and stockholders who found themselves with a rapidly falling company on the stock market. Some Facebook officials distanced themselves from the "breach of trust" invoked by their CEO claiming that users who agreed to participate in surveys, quizzes and all the operations proposed by Cambridge Analytica aimed at obtaining the data accepted terms and conditions of use and therefore they could not complain about their negligence. To run for cover, Mark Zuckerberg wrote an apology letter published sometime later in the form of an ad in the printed editions of the major US newspapers (fig.7)[43], a change in the communication strategy that did not convince users.

Figure 7

In 2018, Social Science One was founded, a Facebook foundation in collaboration with Harvard University, to study models of collaboration between industry and academia.

Meanwhile, Amazon decided to suspend Cambridge Analytica from accessing its platforms and the Italian bank Unicredit to stop digital marketing operations on Meta's platform[44].

- **#DeleteFacebook Movement and The Great Hack**

The public reaction to the scandal was immediate and many protests mainly originated online. The hashtag #DeleteFacebook[45] went viral on Twitter and was also shared by a large number of public figures including the co-founder of WhatsApp, at the time already acquired by Meta, the company that also owns Facebook. However, there were very few who eliminated the application. Research sponsored by the Raimond James Company[46] reported that although 84% of users were concerned about the inappropriate use of their personal data, 48% of those interviewed had no intention of uninstalling the application or reducing their consumption habits. Statistics later confirmed by Zuckerberg himself reporting not large variations in the number of users of the platform.

[43] Stelter, B. (2018, March 25). Tweets. Twitter. Retrieved February 20, 2023, from https://twitter.com/brianstelter
[44] Reuters Staff (2018, August 7). Unicredit has stopped using Facebook for advertising: CEO. Reuters. Retrieved February 20, 2023, from https://www.reuters.com/article/us-facebook-unicredit/unicredit-has-stopped-using-facebook-for-advertising-ceo-idUSKBN1KS1N5
[45] Chen, B.X. (2018, March 21). Want to #deletefacebook? you can try. The New York Times. Retrieved February 20, 2023, from https://www.nytimes.com/2018/03/21/technology/personaltech/delete-facebook.html
[46] The Raimond James Company is an American multinational independent investment bank and financial institution.

To understand why these protests originated online, we should highlight that social media are one of the main tools subject to the so-called network effect. In economics, the network effect is defined as the phenomenon whereby the value or utility associated with the consumption of that specific good or service depends on the number of users and/or consumers already present in the network. Social media fully enjoy this principle. To make an example: if a new social network was to come to the fore and I were to decide to sign up, but none of my friends did, I would have no one to interact with on the platform. Social networks are born with the intention of promoting distance communication, but if the two users are not part of the same system there is no communication possible. This is why movements for the elimination of Facebook are born on the same platform or similar platforms. This is effectively the only way that users have to spread this message. Shrewder was Brittany Kaiser, the former director of Cambridge Analytica, who rather than launching a boycott campaign against Facebook preferred to launch an awareness campaign on the use of personal data under her name (fig.8).

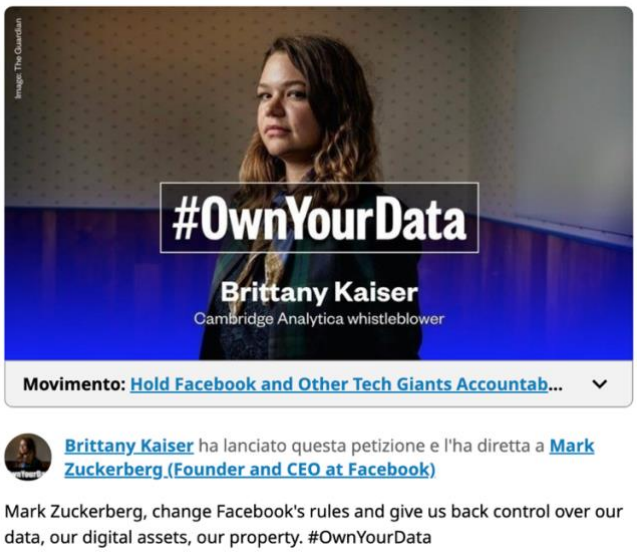


Figure 8

Her #OwnYourData[47] quickly went viral leading to the foundation of the "Own Your Data Foundation"[48] to increase digital intelligence education.

[47] For reference, *see*: https://www.change.org/p/tell-facebook-our-data-is-our-property-ownyourdata
[48] For reference, *see*: https://ownyourdata.foundation/

2. ANALYSIS OF THE INDUSTRY

20 years ago, people had no idea what a social network was. Of course, there were the very first prototypes such as Myspace, the ancestor of today's Facebook, or Live Messenger, the forerunner of WhatsApp. However, these very primordial "social media" were prevalent in a specific demographic, namely that of the younger generation, but above all among those who could afford a personal computer and an internet connection. The technological innovation of infrastructures and access to essential goods for online communication has favored the rapid growth of these services and spread them across all different generations, from Boomers to GenZ. To date, the social media industry has seen exponential growth with a boom starting from the second half of the decade 2010-2020 which marked the rise of the great giants: Facebook, Whatsapp, Twitter and then the more recent Instagram and TikTok. To better understand how social networks are nowadays handling the issue of personal data management and protection, a growing concern among various users, which could cost companies serious losses in terms of finance and brand reputation, we must analyze the functioning of the social media industry and, in particular, of Meta, Mark Zuckerberg's company which plays a significant role within the market.

2.1 THE SOCIAL MEDIA INDUSTRY AS AN OLIGOPOLY

Oligopoly is a very interesting word that derives from the union of two Greek words: *oligos* and *polein*. The first can be translated with "few" while the second with the verb "to sell", the union between them defines this market structure well.

In economics, in fact, the oligopoly is defined as a structure where a market or an industry is characterized by the presence of a few producers who interact with each other. One of the essential characteristics of oligopoly is the interdependence of payoffs[49] which consists in the fact that companies understand that their profit does not depend solely on their production choices, but also on the choices of competitors who can have an effect within the market. As a result, the rival companies will be informed of a firm's market activity and will react accordingly. This means that while considering a market action, a firm must take into account all potential responses and countermoves from rival enterprises[50].

This is why, when we talk about oligopoly, we need to apply the key concepts of game theory and we talk about best response functions in terms of the behavior of every single company on the market.

[49] Melvin & Boyes, Microeconomics 5th ed. page 267. Houghton Mifflin 2002.
[50] Colander, David C. Microeconomics 7th ed. Page 288 McGraw-Hill 2008.

Before addressing the further characteristics of oligopoly and analyzing them accordingly, it is important to make a first distinction between perfect and imperfect oligopolies. An oligopoly is said to be perfect, or pure, when the goods produced by the companies present in the reference industry are homogeneous which, translated, means that they are identical or have very similar characteristics such as to determine a high degree of interchangeability. Hence, it follows that in a pure oligopoly the elasticity of the substitution approximates infinity[51]. These types of oligopolies are frequent in industries where companies have strong homogeneities such as the agriculture and food industry in which, assuming that the price of the same good is identical for all companies, a rational consumer would be indifferent in choosing the product. For instance, if there are 5 companies that produce apples and each company sets a price of 1 euro for each apple, the consumer will be indifferent in his choice of consumption, i.e., he will not have preferences for any of the 5 companies. On the other hand, imperfect (or, sometimes, differentiated) oligopoly is defined as the case in which the companies present within the market produce goods that are heterogeneous in their nature, i.e., goods that do not share any characteristic, if not of negligible entity, and they are not interchangeable with each other. Generally, this type of oligopoly is frequent in the manufacturing and service industries where differences in the production method decree substantial differences in the quality or features of the products placed on the market. In this case, the elasticity of substitution generally depends on the personal characteristics of the consumer and on the product under consideration[52]. Another peculiarity of the oligopoly, as a market structure, is certainly the presence of high entry barriers. We define barriers to entry as factors that prevent new companies or enterprises from entering the market, significantly limiting the level of competition and acting as dissuaders for entrepreneurial development[53]. Some of the most frequent barriers to entry are the high start-up costs (especially in the case of companies that enter the production of innovative products or services), government licenses and the stringent regulations of the reference sector as well as the economies of scale i.e., those cost advantages which are generally obtained when production becomes efficient and which are difficult to reach in the short term for a new-born company and, lastly, costs and access to the right technology to penetrate the market. Although it rarely happens, there are some peculiar cases in which the barriers to entry are almost nil or non-existent and, in that case, we speak of open oligopoly. On the other hand, a closed oligopoly is an oligopoly where the barriers to entry are extraordinarily high and where new competitors are unlikely to arise. These barriers, in addition to preventing a significant increase in competition, also allow companies to ensure a certain market power that they

[51] Stigler, George J. (February 1964). "A Theory of Oligopoly". The University of Chicago Press Journals. 72(1):44–61 – via JSTOR.
[52] *Id.*
[53] Hirschey, M. Managerial Economics. Rev. ed, page 451. Dryden 2000.

can exercise on prices and more easily achieve their goal of maximizing profit[54]. We mentioned, at the beginning of the paragraph, how one of the cornerstones of oligopoly is the interdependence of the payoffs. Companies are aware that to survive in the market or in the industry they must also take into consideration the actions of their competitors. It is not said, however, that they have all the information they need at their disposal. Assumptions about perfect knowledge vary from model to model, but we can generally agree that the level of information companies have access to is selective. Every firm that is part of an oligopoly certainly has perfect knowledge of its own cost and demand function, but information about other firms may be incomplete. However, if companies decide to collude in the market, then this information could - because it doesn't necessarily happen, every company could decide to cheat - become more accurate. Net of this, we could define the social media industry as a very particular oligopoly since it retains some of the most basic characteristics such as the presence of few companies on the market and the desire to maximize profits, but it is hybrid in its nature. We cannot actually say it is either a pure or differentiated oligopoly since services companies offer cannot be defined as either totally homogeneous or totally heterogeneous. The main intention of a social media is to connect people to each other in a virtual space of social aggregation (which represents a homogeneous goal for all social media) and, very often, even the features offered are very similar between of them (think of the fairly common possibility of sharing photos, posts and videos), however social networks are heterogeneous in the audience of users they attract, as we will discuss in the following paragraphs. Plus, examining further the possibility of colluding, we will soon discover that, as far as the social media industry is concerned, collusion does not make much sense.

2.2 WHY COLLUSION IS NOT POSSIBLE

First, we should start by analyzing the definition of collusion and why companies decide to collude within an oligopoly.

Collusion can be defined as the conduct intended to coordinate the actions of firms. It basically requires an agreement that must be reached by the firms involved and this agreement can be explicit, when stated in official documents or overt communications, or implicit (also called tacit) when there is no explicit or recorded communication between firms. Given these premises, companies would become interdependent with each other, and this would be the basis for their strategic interaction. There is one problem and that is that companies could always find it convenient to cheat at some point in the game to maximize its profits at the expense of the opponent.

[54] Osborne, Dale K. (August 1964). "The Role of Entry into Oligopoly Theory". The University of Chicago Press Journals. 72(4):396–402 – via JSTOR.

This problem is often defined as *cheating problem* and one of the proposed solutions is that of repeated interaction.

George Stigler, Nobel Prize for Economic Sciences in 1982, analyzed how the enforcement of a collusion agreement essentially depends on three factors:

- **Detection:** firms can identify if competitors have secretly cheated.
- **Speed of punishment:** it must deal with how fast firms can actually realize (and punish) that competitors cheated.
- **Strength of punishment:** it must deal with how harsh the punishment is when imposed to cheaters.

To better understand, consider the following example.

Suppose there are only two firms in the market, firm A and firm B, and that they compete for two periods.

The strategies of the two companies could be summarized as follows:

- In period 1, firms are supposed to cooperate producing each half of the monopoly output.
- In period 2, firms are supposed to cooperate in producing the Cournot level of output[55], unless one of the two has cheated in the first period leading the other one to produce the competitive level of output.

In this case, the monopoly output can be considered the first period's Nash Equilibrium. If either one of the companies decided to cheat in the first period, it would end up with zero profit in the second period and this is a strong deterrent from avoiding cheating.

However, the threat of punishment in the second period is not credible. If either firm decides to cheat in the first period, all that is left to do in the second period is to both produce the Cournot level of output. The situation changes if the two companies decide to play a supergame, i.e., a game that can be played infinitely.

In this case, companies have two strategies they can apply:

- They can decide to apply the *collusive path* which basically means playing the collusive output at every stage as long as the other firm does so.
- They can also decide to apply the *punishment path* which basically means deviating from playing the collusive output and punishing the cheating firm by playing the Cournot output.

[55] By definition the Cournot level of output is always lower than the monopolist's one.

Apart from firms' behaviors, there are also some other factors that influence the sustainability of collusion, and these are:

- **Public Prices:** they facilitate collusion since it is much easier to detect cheating from firms.
- **Size of the cartel[56]:** more firms are in the cartel, lower is the firm's share in the collusion profits, hence more incentives to cheat.
- **Product differentiation**
- **Multimarket contact:** in this case collusion can be spread to other markets.

Now, applying all these concepts to the social media industry, collusion is not possible.
Collusion is closely connected to the fact that the cooperation is beneficial for both companies. This is a principle applicable to the vast majority of consumer goods and services, but certainly not to social networks. If company A and company B produce apples, it will certainly be convenient for them to cooperate from the moment in which the consumer requests a well-defined total quantity of apples, but above all, if the prices are different, he would buy the apples from the one offering the lowest price. As far as social networks are concerned, these tend to have no price, so that a consumer could sign in on several social networks at the same time. But above all, the fact that a consumer subscribes on a social network does not affect another's audience of users. For example, a user could decide to sign up for Facebook and Twitter at the same time. Subscribing to one of the two social networks does not exclude subscribing to the other.
It, therefore, makes no sense for companies belonging to the industry to start cooperating, since they would not derive any benefit from it. But there is another aspect that needs to be taken into consideration.
Since it is true that presence on multiple platforms is possible and that the profit of each individual company depends on the number of users it attracts, then every company has the goal of attracting as many users as possible to its platform. Social networks are subject to another curious phenomenon, namely that of a *natural targeting*.
Among the habitual users of social networks, it has spread the idea that some platforms are more inclined or suitable for some specific age groups[57].
For instance, Facebook is considered a social network for Boomers and Generation X, while Instagram has met the taste of Millenials and GenZ over time. It is as if these platforms had polarized around a specific target which leads to the exclusion or, at least, lower participation of the others.

[56] A cartel is a group of firms that have an explicit agreement to reduce output in order to increase price.
[57] For reference, *see*: Kowalewicz, R. (2020, January 9). Council post: What to consider for generation-based social media marketing. Forbes. Retrieved February 24, 2023, from https://www.forbes.com/sites/forbesagencycouncil/2020/01/09/what-to-consider-for-generation-based-social-media-marketing/?sh=1d7269524242

This represents an important threat for social media companies which over time have had to develop new tactics to make themselves appealing to adjacent customer segments. A strategy has been devised by Facebook which since 2012 has begun to engulf its competitors through acquisition processes. These mergers gave birth to what is now called Meta, and which owns four of the most used social media in the world.

2.3 MERGERS AND ACQUISITIONS BY META

It could be said that mergers and acquisitions have existed since the birth of companies and that, since the dawn of entrepreneurship and the development of markets, they have always represented a valid corporate tool. From the nineteenth century, mergers have occupied a significant space within a company's strategy allowing it to exploit economies of scale, competitive advantage and to expand the size of its production and trade. To date, mergers and acquisitions, which are very often referred to by the term M&A, are defined as transactions of a financial nature where the ownership of companies, other business organizations or operating units is transferred or consolidated within another company[58]. Since mergers make it possible to redefine the shape of a company, both upwards and downwards, they play a fundamental role in corporate strategy. The purchase of a corporation or business by another firm or other commercial entity is referred to as an acquisition or takeover. Market research, trade shows, internal business units, supply chain analysis, and other methods may all be used to discover specific acquisition targets. The assets or ownership stock of the acquired firm may be purchased at 100% or almost 100% in this way. A consolidation (or amalgamation) takes place when two businesses merge to form a new enterprise in which neither of the previous enterprises stays independent. Acquisitions are classified as "private" or "public" based on whether the acquiree or merging company (also known as a target) is or is not listed on a public stock exchange. Acquisitions are an important value-creation strategy for some public companies.
Another dimension or classification is whether an acquisition is friendly[59] or hostile[60]. There are three types of mergers to consider, which have distinct characteristics and objectives from each other.

[58] Bainbridge, S.M. (2020). Mergers and Acquisitions. In Corporate law (pp. 410–412). Book, Foundation Press.
[59] In a friendly acquisition, the target company's board of directors (or management) approve the takeover proposal and help to implement it.
[60] In a hostile acquisition, the board of directors (or management) of the target company opposes to the takeover.

These are:

- **Vertical mergers**: when multiple companies, operating at different levels within an industry's supply chain, combine their operations, particularly along the production and distribution process of a business. This category essentially exploits the idea of creating something greater than the sum of the two combining companies. As a result, the operations' efficiencies improve, resulting in stronger and higher quality control and, ultimately, advantages out of an improved information flow along the production process. As a result, the company pursuing this merger strategy gains full control over its supply chain. Indeed, generally vertical mergers involve the acquisitions of the key suppliers[61] with the distributors and the retail locations. However, some vertical merger cases demonstrate that this type of transaction can occur even when the two firms are not competitors, but convergence makes logical sense.

- **Horizontal mergers**: arise from the combination of two competitors in the same industry. Companies decide to acquire their rivals for multiple reasons, but the best known and most shared is to acquire greater control of the market and strengthen their leadership as well as expand the category of services or products offered to the consumer. In doing so, the company can combine the product lines and assets of the two companies, expanding the potential flow of customers and the competitive advantage in the sector.

- **Conglomerate mergers**: are those mergers where the merging companies are part of completely unrelated industries or lines of business. They are then divided into pure conglomerate mergers and mixed conglomerate mergers. The former, as the word may suggest, has to do with two completely unrelated companies. The latter, on the other hand, has to deal with companies that use the merger to be able to expand their product line or avoid the entry barriers of a particular market or industry. Sometimes, one of the strategies used to facilitate entry into the market is precisely that of acquiring companies that are already present, in such a way as to avoid a series of implicit and explicit costs. Generally, these types of mergers are adopted by very large companies headed by smaller companies operating in various sectors. One of the most classic examples is that of Unilever, a company that owns a large number of brands ranging from food production to personal and home care products.

[61] In this case, there is a *backward integration* while, if the company buys a former customer, we talk of a *forward integration*.

M&As are often reviewed by judicial authorities to verify that they do not actually affect market competition in favor of companies that could achieve a certain level of monopolistic power and therefore do not have a negative effect on consumers. In Italy, this operation is conducted by the Italian Competition Authority, while in the US by the Antitrust division of the Department of Justice. The competition authorities only examine mergers that exceed a certain threshold, and this can be done by applying two tests. A substantive test is first performed which allows authorities to determine whether there has been the creation or reinforcement of a dominant position or whether there have been significant impediments to competition. Subsequently, however, there is the implementation of a counterfactual analysis where a comparison between the competitive conditions that would emerge both if the merger was completed and in the event that this did not occur in the market is made. In most cases, the competition conditions present at the time the merger takes place represent the most relevant comparison for evaluating the effects of a merger. The analysis must also take into consideration the possible entry and exit of companies from the industry in the event that the merger did not take place, which means developing market forecasting models. Another aspect to take into consideration when evaluating a merger is efficiency. The analysis of these claims could lead to the conclusion that following a series of efficiencies deriving from the acquisition, the merger cannot be declared incompatible with the law. However, efficiencies must cumulatively benefit consumers, be merger-specific, and be verifiable by the competition authority.

Initially, all acquisitions of the Facebook group had been acquisitions of a horizontal nature. To be precise, the main intention of Mark Zuckerberg, CEO of the platform, was to carry out "talent acquisitions" where acquisitions are meant with the aim of being able to recruit the staff of a company, and therefore acquire talents and professionals in the sector. In one of his very first interviews in 2010 Mark Zuckerberg would have stated in this regard: "We have not once bought a company for the company. We buy companies to get excellent people... In order to have a really entrepreneurial culture one of the key things is to make sure we're recruiting the best people. One of the ways to do this is to focus on acquiring great companies with great founders"[62].

All the acquisitions between 2010 and 2012 have common characteristics that can highlight how Facebook's corporate strategy was still very primordial and inclined to increase the size of the company rather than rise toward a dominant position in the market. The companies acquired were mostly startups in development or that would have met bankruptcy had they not been taken over by the company. In 2009 Mark Zuckerberg launched a question on Quora[63], the well-known question-

[62] Mark Zuckerberg (2010, October 18). Why Facebook buys startups. YouTube. Retrieved February 25, 2023, from https://www.youtube.com/watch?v=OlBDyItD0Ak&ab_channel=BizBuzz

[63] Zuckerberg, M. (2009). What startups would be good acquisitions for Facebook? Quora. Retrieved February 25, 2023, from https://www.quora.com/What-startups-would-be-good-acquisitions-for-Facebook

and-answer site that has gradually replaced the late Yahoo Answer!, asking users which startups could have been good acquisitions for Facebook. By doing this, Zuckerberg marked a turning point in business management by creating a point of contact between his company and the needs of consumers and then acting accordingly. The question did not actually achieve great popularity at the time, reporting 79 answers, much less than it would receive today, but it remains one of the most clicked and sought-after questions on the platform even today.

This behavioral pattern changed in 2012, the year in which Facebook announced the acquisition of Instagram for one billion dollars. The acquisition of Instagram marked one of the turning points in Facebook's strategy but above all, the beginning of its competitive ascent. From 2012 onwards, Zuckerberg continued his strategy by alternating talent acquisitions with product-focused acquisitions, so that in 2014 he acquired WhatsApp and OculusVR, the augmented reality company with which Zuckerberg will test the Metaverse. Facebook finds itself today with 4 of the most important social media networks on the world scene[64], marking a risk that it is achieving a competitive advantage such as obtaining an almost monopolistic control of the market through this acquisition strategy.

2.4 MERGER REVIEW AND THE THREAT OF DATA

A merger can have a significant effect on the competition of a market by facilitating the removal of some important competitive constraints against one or more producers, increasing the market power of the merged firm. One of the direct effects that can be observed right away is the reduction of the competition between the two merging firms. From the very moment in which, in a horizontal merger, the two merging firms merge to become a single legal entity, they are no longer in competition with each other. In addition, they acquire all the resources of each other and therefore also the audience of existing and potential customers. Among other things, a merger does not necessarily lead to the unification of the two brands; especially in the social networks industry, the two brands remain present and well-defined but fall within a broader umbrella of the group that owns them. To give a practical example, after the acquisition by Facebook, the social Instagram has not changed its name or form, however, it has started to be part of the company Facebook Inc. (the future Meta Inc.), which is why whenever Facebook’s database does not work, this also has an effect on the possibility of using Instagram.

Nonetheless, it is not said that non-merging firms are necessarily disadvantaged by the acquisition, in some cases, they could even benefit from it. Sometimes, the reduction of competition can be

[64] Kepios. (2023, January 1). Global Digital Report 2022. Kepios. Retrieved February 25, 2023, from https://kepios.com/reports

beneficial since the merger could produce a change in the demand of the merged entity which would fall on rival companies, and they could find it profitable to increase the prices of their goods or services. In such situations, the only ones who do not benefit are the customers who find themselves with a reduction in their welfare, which is why the intervention of the competent authority is absolutely necessary. There are mainly two ways in which a horizontal merger can significantly impede competition. On the one hand, the merger could produce unilateral effects that consist in the elimination of the competitive constraints of one or more companies ending up with an increase in market power. On the other hand, the merger could generate coordinated effects that would be reflected in the change in the competitive nature of the market such that companies that previously did not coordinate their market strategies would now be inclined to play strategically to raise prices. Effects of this kind can also benefit the coordination of companies that were already colluding in the market.

Mergers in oligopolistic markets that deal with the elimination of important competitive constraints could, even in the case where the probability of coordination is low, favor a significant impediment to competition. Most of the time, merging firms brag and try to convince the antitrust authorities about the positive effects that a merger would have by taking into consideration the efficiencies it would generate for the merging firms. By exploiting complementary assets or cost synergies, a new entity would be much more efficient from a production point of view, which technically should benefit consumers who would find themselves faced with greater product availability and a basically lower price given the reduction of production costs. Should this happen, the antitrust authority would have no reason to intervene. When it intervenes it is because, as said before, companies, experiencing an increase in their power, have reduced consumer welfare. Most countries around the globe have their own National Competition Authority, and each country has developed merger evaluation systems that may or may not be in line with national standards. The European Union has adopted a regulatory system that includes both the European Commission and the national authorities of the 27 member countries of the Union which cooperate thanks to the European Competition Network[65]. The latter serves to guarantee cooperation between the nations of the Union, so that the competent authorities can exchange the information necessary to be able to correctly evaluate the mergers and carry out particularly careful and meticulous analyses. The United States of America, on the other hand, have adopted a body at the federal level, the Federal Trade Commission which belongs to the Department of Justice, and which collaborates with the latter in order to be able to evaluate the legitimacy of an acquisition. The procedures adopted in the US and in Europe are almost similar. In Europe, the merger review procedures consist of 6 steps which are followed by the EC and the

[65] For reference, *see*: https://competition-policy.ec.europa.eu/european-competition-network_en

competent national authority. First, as reported on the European Commission website[66], only very large mergers with an EU dimension are examined, i.e., mergers that exceed a certain turnover threshold. There are six thresholds that are reported: (i) a combined worldwide turnover of all the merging firms over €5.000 million, (ii) an EU-wide turnover for each of at least two of the firms over €250 million, (iii) a worldwide turnover of all the merging firms over €2.500 million, (iv) a combined turnover of all the merging firms over €100 million in each of at least three Member States, (v) a turnover of over €25 million for each of at least two of the firms in each of the three Member States included under iv, (vi) EU-wide turnover of each of at least two firms of more than €100 million. If the merger does not reach the EU dimension determined by these thresholds, it will be examined only by the national authorities.

The first step adopted by the EU concerns notification. The commission must be notified of any merger that has EU dimension before its implementation. If the merging firms do not operate in the same market (or in similar markets) or if they have very small market shares such as not to reach specific market share thresholds, generally the merger should not give any kind of problem and a simplified procedure is applied. In the event that the thresholds are exceeded, the commission adopts an investigative procedure. The second step has to do with the investigation. Following notification, the Commission has up to 25 working days to review the merger. Generally, this first phase involves the request for information from the merging firms or third parties and the questioning of competitors and customers to determine their point of view on the mergers as well as the clarification of the competitive conditions of the market and the role of merging companies in that market. The Commission keeps the merging companies informed throughout the investigation phase, at the end of which the merger can be declared unconditionally cleared or subject to remedies to be accepted or else the investigation may have brought to light the risks for competition that would lead the Commission at the opening of the second investigative phase. Let us consider for a moment the possibility that the merger has been cleared and analyze what remedies can be imposed by the Commission.

If the Commission believes that there may be a risk to market competition, it could ask the merging firms to offer remedies (also called commitments) to ensure competition. These can be proposed both in phase I and in phase II of the investigation and are analyzed by the Commission also through a market test, i.e., a test that serves to take into consideration the point of view of the other market participants. If the remedies are accepted, an independent trustee is appointed to ensure that these are complied with. If instead the second phase of the investigation proceeds, the Commission will undertake an in-depth analysis of the effects of the merger on competition. Usually, this phase

[66] https://competition-policy.ec.europa.eu/system/files/2021-02/merger_control_procedures_en.pdf

involves a longer processing time and the request for more information from the companies as well as the acquisition of external documents, economic data, and site visits. In phase II, the Commission then analyzes in detail the claimed efficiencies that would be achieved thanks to the merger and in the event that the benefits for consumers outweigh the negative effects, then the merger would be cleared. However, these efficiencies must comply with some strict conditions including verifiability, merger-specificity i.e., they cannot be achieved except through a merger, and they must be passed on to consumers i.e., their positive effect must be reflected on consumers. If the Commission considers that the merger represents an obstacle to competition, it sends a Statement of Objections (SO) to the interested parties who can respond within a certain period and request an oral hearing.

After that, the Commission has 90 working days from the opening of phase II to take a final decision on the basis of the EU Merger Regulation. Some extensions to this rule may be granted in the case of particular situations, but the Commission has the main interest of aligning its timing with those of other international authorities to favor more efficient cooperation. The final decision, which follows the second phase of the investigation, may lead to the unconditional clearance of the merger, the approval upon remedies implementation, or the disapproval of the merger if no adequate remedy has been proposed. All final decisions are then officially published with the sensitive information of the companies involved removed. Ultimately, all decisions and procedures adopted by the Commission are reviewed by the General Court or the Court of Justice. Companies can appeal the decision within 2 months of its publication. The judicial review is an indispensable process to ensure that the rights of companies are respected and that there has been legitimacy of the investigative process.

Taking into consideration the American system, it is necessary to refer to the Hart-Scott-Rodino (HSR) Act according to which some large mergers or acquisitions need to file a premerger notification and wait for the government review before being able to consider the transaction concluded. Also in this case there are five steps to follow[67]. First, you need to file the notice of a proposed deal in case the merger exceeds a certain threshold and sometimes some stocks or assets are exempt from counting. The data must be forwarded by both the buyer and the seller and once this procedure has been completed, the parties must wait 30 days (or 15 if the merger is used to save a company from bankruptcy or in the case of a cash tender offer). The second step is that of clearance by an antitrust agency. The file is forwarded to both the Department of Justice and the Federal Trade Commission, but only one of these two agencies will review the proposed merger. The two agencies generally consult and may conclude with clearance of the merger or additional review by the other agency. The third step has to do with the expiration of the waiting period or the second request from the agency.

[67] Staff, the P.N.O., &; Nguyen, S. T. (2022, March 4). Premerger notification and the Merger Review process. Federal Trade Commission. Retrieved February 26, 2023, from https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/mergers/premerger-notification-merger-review-process

After the preliminary review of the merger, the agency in charge can decide to declare the merger cleared before the end of the waiting period (grant "Early Termination" or ET), wait for the waiting period to end, or request additional information (the so-called "Second Request") to each party involved. If the waiting period ends without the agency requesting further information, the parties are free to terminate the agreement. The second request is the equivalent of the second European investigative phase where additional information is requested from the two companies. In the fourth step, the two companies have the duty to facilitate the investigation by providing all the necessary materials and the agency has an additional 30 days to review all the documents (10 in the case of a cash tender offer or bankruptcy). This time may be extended if there is an agreement between the parties and the government to resolve any disputes without resorting to litigation. The last step, the fifth, leads us to the closure of the investigation and the final decision. This could lead to the authorization to continue with the merger, to a negotiated consent agreement with the companies with provisions (the equivalents of European remedies) to encourage healthy competition, or the refusal of consent to the entire transaction. As regards the mergers carried out by Meta, these were very often subjected to the analysis of the competent authority, which in most cases determined that there were no problems relating to centralization of market power in the hands of the company nor least of all a problem for the competitors on the market[68]. However, the real problem with these mergers, as it has been reported by numerous scholars and newspapers, is that all user data would fall within a single server, that of Meta, and this could represent a big problem if the servers in question should be hacked or, even worse, the data should be exploited by third-party companies operating on the platforms. This is why governments have moved towards a more stringent regulation that obliges social media companies to implement operations for the protection of personal data in compliance with the General Data Protection Regulation, also known by the acronym GDPR. Operations which, however, are not always performed in the clearest and most linear way possible for users.

[68] One of the latest decisions has been taken on the February 1, 2023. For reference, *see*: McCabe, D., & Frenkel, S. (2023, February 1). Judge is said to let Meta's virtual reality deal move forward. The New York Times. Retrieved February 26, 2023, from https://www.nytimes.com/2023/02/01/technology/meta-within-deal-ftc.html

3. DATA PROTECTION POLICIES COMPLIANCE

Years before the Cambridge Analytica scandal came to light, central governments of the major Western countries had asked themselves questions and cultivated doubts about the power that the enormous amount of data poured into the databases of social media companies could have given them. Over the years, the central authorities have begun to launch a series of national provisions regarding the use and protection of the personal data of users entrusted to the supervisory authorities who are responsible for supervising the work of public and private companies. However, the real turning point came in 2016 when the European Union launched the first General Data Protection Regulation, better known by its acronym GDPR, surpassing the Data Protection Directive of 1995.

3.1 EUROPEAN REGULATIONS

- **Data Protection Directive and previous attempts**

The Data Protection Directive, officially known as Directive 95/46/EC, laid the foundations for what would later be the GDPR. Issued in October 1995, it is a European Union directive concerning the regulation of personal data within the European Union territory- therefore not only for companies that have their registered office in the territory of the Union, but for anyone operating within the Union itself - and the arrangement of this data.
The foundations on which this directive is based are the right to privacy which is recognized as one of the fundamental human rights and the *European Convention on Human Rights* [69] of which all member states of the Council of Europe are signatories and which in article 8 inserts the right to respect private correspondence and inserts a series of restrictions and limitations to ensure privacy. It is important to underline that, at the time of the European Convention on Human Rights, we actually spoke only of correspondence since the convention was drafted in 1950 and entered into force in 1953, almost 40 years before the birth of the World Wide Web. However, this was fundamental for recognizing the right to privacy as a cardinal right of the private citizen which, according to the Union, had to be necessarily protected. A second effort took place in 1980 when the Organization for Economic Co-operation and Development, better known as OECD, in an attempt to create a comprehensive and unified personal data protection system for the whole

[69] Council of Europe. (1950, September 3). European Convention for the protection of human rights and fundamental freedoms. Wikisource, the free online library. Retrieved April 11, 2023, from https://en.wikisource.org/wiki/European_Convention_for_the_Protection_of_Human_Rights_and_Fundamental_Freedoms A full copy of the text can be found at this link.

European territory, released a document entitled *Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data*[70] which is a document containing the guidelines on the processing of personal data. The Committee for Information, Computer and Communications Policy recommended that member nations cooperate across borders in the enforcement of laws protecting privacy by inviting them to improve domestic frameworks for privacy law enforcement trying to unify national regulations in such a way as to guarantee international cooperation, develop international mechanisms to facilitate cross-border enforcement and make stakeholders - i.e. citizens - aware of privacy protection activities and the risks deriving from the uninformed release of data.

The seven principles that governed the OECD recommendations were:

1. ***Notice*** = notice should be given when data are collected.
2. ***Purpose*** = data are meant to be used only for the stated purpose.
3. ***Consent*** = no data can be disclosed or used without consent.
4. ***Security*** = data should be kept secured from any potential abuse.
5. ***Disclosure*** = citizens should be aware of who is collecting their data.
6. ***Access*** = citizens should be allowed to access their data.
7. ***Accountability*** = data collectors should be held accountable for legal actions if they do not follow the principles.

The recommendations were implemented by almost all OECD member countries, even though the United States was largely absent and, while approving and accepting the recommendations, never did anything to implement them. A problem, however, soon arose in Europe. Since the recommendations were non-binding - meaning that each state could decide either not to implement them or to have implemented them in the way it deemed most appropriate and in line with its own legislation - these generated a series of different national regulations which came into conflict with the cardinal principle that guided the work of the Council, namely that of international cooperation and the simplification of bureaucratic processes. A second attempt was made in 1981, when the member states of the Council of Europe adopted the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*[71] also known as Convention 108 which

[70] OECD. (1999, January 5). Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data. OECD Legal Instruments. Retrieved April 11, 2023, from https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

[71] Council of Europe. (1981, January 28). Council of Europe Convention No. 108 on Data Protection. European Data Protection Supervisor. Retrieved April 11, 2023, from https://edps.europa.eu/data-protection/our-work/publications/legislation/council-europe-convention-no-108-data-protection_en

resumed the 1950 convention updating it in terms of legislation for automated personal data management processes. The industrial boom of 1960 had led to a modernization of production processes, prompting numerous companies to incorporate the very first, and still not very efficient, digital archives into their business processes, which is why the Council of Europe soon felt the need to modernize the 1950 convention. A subsequent modernization will take place in May 2018, a few months after the Cambridge Analytica scandal, when the agreement will be enriched with more stringent legislation in the case of data breaches and an additional accountability for data storers. It is within this context made up of attempts, approximate solutions and communication problems that the *Data Protection Directive*[72] was born. First, the most significant change occurred in the mode of diffusion. A directive rather than a convention or recommendations must necessarily be adopted by the member states of the Union in a well-defined period, while leaving each individual state free to legislate as it sees fit. However, all laws or legislative adoptions are always submitted to the careful judgment of the Commission which, if it deems the directive has not been adopted in a complete way, can request improvements or legislative adjustments. Beyond the legislative form, the Data Protection Regulation breaks the pattern of the past by providing in article 2 of chapter 1, dedicated to the general provisions, a series of definitions necessary and absolutely essential in the management of personal data. Defining the object of the directive has made it possible to clarify the matter in question and to limit the scope of action of the competent authorities.

For the European Union, personal data is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"[73].

The natural person is not identified exclusively for his connotations, but also for the personal characteristics relating to the cultural and social sphere. One aspect to highlight is the use of the adjective "physiological" which therefore also determines the data relating to the individual's psychometric characteristics which, as seen in the first chapter of this thesis, have determined one of Cambridge Analytica's peculiar methods of action in terms of the exploitation of personal data. Therefore, even the OCEAN tests we mentioned earlier fall within personal data. This definition remains very broad in order to embrace all possible cases where someone is capable of creating connections between the data obtained and the data subject.

[72] European Union. (1995, October 24). Data Protection Directive 95/46/EC. EUR-Lex. Retrieved April 11, 2023, from https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A31995L0046 A full copy of the text in multiple languages can be found at this link.

[73] *Id.*

Secondly, the processing of personal data is defined by the directive as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction"[74]. Also interesting in this case is the concept of "alignment or combination" which is reported by the definition. It will be precisely the combination of personal data through micro-targeting operations to constitute one of the breaches of Cambridge Analytica's case. Responsibility for compliance with this data rests with the person defined as the "controller" i.e., the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law even if there should be a "processor" or "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller"[75]. Furthermore, in compliance with the rules of the past, the data protection rules are applicable not only when the controller is physically based in the European Union, but also when he - or whoever the processor is - use equipment located in Europe for processing personal data.
More generally, any controller located inside or outside the EU and processing data in the EU must necessarily follow the data protection regulation of the country where his business is located. The principles that guide the directive are those of transparency, legitimacy and proportionality which also determine the conditions such as to decree the possibility of processing personal data.
The principle of transparency is reported in articles 10 and 11 according to which the member states must provide that the controller or whoever acts on his behalf - in the event that there is a representative - must provide the data subject with information about the identity of the controller, the reasons why the data processing takes place as well as the existence of the right to access or rectify the data provided (art.10). In case, however, the data has not been obtained directly from the data subject, but rather from third parties, the controller must ensure that the data subject is aware of the identity of the controller, of the fact that his data will be used by the controller and for what purpose and in the same way give the right to access and rectify the data (art.11). In addition to these two articles, subparagraph (a) of Article 6 provides more generally that data be processed in a fair and lawful manner.

[74] *Id.*
[75] *Id.*

The legitimate purpose instead occurs in the event that at least one of the following conditions should be respected as reported in Article 7:

i. the data subject has given his unambigous consent.
ii. data processing has a specific purpose (such as entering into a contract).
iii. processing is necessary for compliance with a legal obligation.
iv. processing is necessary to safeguard the interests of the data subject.
v. processing is necessary for purposes of public interest.
vi. processing is aimed at the legitimate interests of the controller or someone on his behalf, except in the case in which these go to harm the fundamental rights and freedom of the data subject.

Finally, the concept of proportionality is summarized in paragraphs (c) and (d) of Article 6 which specify how personal data must be "adequate, relevant and not excessive in relation to the purpose for which they are collected and/or processed" (art.6c) and "accurate and kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed , are erased or rectified" (art.6d). In addition, in the event that personal data concerning information on ethnic or racial origins, opinions of a political nature, religious or philosophical beliefs as well as data concerning the state of health or sexual life of the data subject are processed, greater restrictions and limitations are applied as highlighted in article 8.
Directive 95/46/EC on the protection of personal data was adopted and transposed by individual states by the end of 1998. On 25 January 2012, the European Commission announced its intention to unify the data protection law among the various European nations through a specific legislation called the General Data Protection Regulation improving the corporate data transfer rules with countries outside the European Union (at the time regulated by the directive which provided in a very general way that the transfer of information was allowed only if the country of arrival of the information guaranteed an adequate level of protection of personal data, a provision that was too vague) and to improve user control of personal data.

- **General Data Protection Regulation (GDPR)**

In December 2015, the General Data Protection Regulation was voted on by the members of the European Union with the intention of replacing the old Data Protection Directive. The latter, although it had worked well in the years of its establishment, was now behind the times and therefore did not provide an effective key to the protection of personal data net of the most modern

technologies. The GDPR, therefore, does not represent a real radical change, but rather an adaptation to more recent times, which is why in this paragraph only the differences with its predecessor will be addressed and examined.

First of all, if the DPD was presented as a directive whose implementation method was therefore left to the individual states, the GDPR is released as a regulation therefore it is directly binding and applicable, which means that it cannot be reworked or modified by national governments. However, even this leaves a small margin of flexibility and adaptation where foreseen in the articles of the regulation.

One of the most significant changes made in the GDPR concerns the definition of personal data. 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, in particular by reference to an identifier such as a name , an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"[76]. The big difference with the past would consist in the introduction of a series of factors not previously contemplated such as "online identifiers", i.e., IP addresses, mobile device identifiers and geolocation as well as data of a genetic nature such as, for example, biometric data which commonly we use nowadays to unlock our devices. This change in definition is actually very important as it reflects technological transformations, and the way data is collected and processed by companies. Therefore, by limiting the use of this data, the Union also intends to limit profiling tactics.

Secondly, the GDPR aims to give anyone residing or located in the European territory to have greater control and access to their information. An opt-in mechanism has therefore been established for which the data subject (whose definition remains the same as the DPD) must expressly consent to the processing of personal data. The so-called cookies, which appear to us every time we visit a web page, were born with this exact purpose, namely, to guarantee that the opt-in mechanism is respected and that the consent is informed, unambiguous and user specific. Furthermore, cookies must be customizable, i.e., the user can decide to opt-in only for some of his personal data and deny consent for others.

In support of the data subject then there is also a second ancillary right, the right to access the data provided. Let's say I visit any website and, by mistake, accept all cookies without selecting only those of my interest. At that point, I do not have any idea of what data I have released to the data controller, but I can always get it by requesting the controller information about the use and

[76] Privacy Guarantor. (n.d.). GDPR - Regulation 2016/679. GDPR - Regulation 2016/679 - Privacy Guarantor. https://www.garanteprivacy.it/regolamentoue

methods of data collection. All must then be accompanied by an electronic copy of the data provided, all free of charge. If, following this procedure, the data subject deems it appropriate, he can always request his data to be eliminated from the database. So, to go back to the previous example, I could ask the website manager, or whoever he is (the so-called processor), to delete my data from his database and he could not object.

Speaking precisely of data controllers and data processors, the GDPR introduces a great novelty also in this field. First of all, the new regulation aims to provide a more accurate description of the data processor which is identified as: "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"[77]. But above all, if with the DPD only data controllers were held accountable for the incorrect use of data, with the adoption of the GDPR also data processors are held liable for the security of personal data. A Data Protection Officer (DPO) is appointed to control these two figures if the core activities of the controller or processor have to do with "regular and systematic monitoring of data subjects on a large scale"[78]. This person, who can also be an employee of the company, must be kept updated on the processing and storage of personal data by the controllers and processors and must carry out assessments in the event that he believes there is a high risk of data breach from part of the company.

In the event that a data breach occurs, for example following a cyber attack, the DPD provided that every nation in the European Union could provide for breach notification laws. However, this had generated a chaos of different laws by asking companies that had suffered a data breach to verify if they complied with the legislation of each individual state. The GDPR, from this point of view, aims to harmonize everything by requiring only one rule to be respected. The data controllers are therefore asked to notify the authorities, within 72 hours of the data breach, providing a series of information such as the nature of the breach, the category and the approximate number of data subjects involved and the contact details of the Data Protection Officer. In addition, it is required that the consequences deriving from the data breach and the respective actions aimed at mitigating everything are estimated. The controller is then required to inform individuals about the data breach whether this represents a risk to the rights and freedoms of individuals without undue delay.

In our reference case study, Facebook promptly informed users about the risk of personal data misappropriation by the British company once it discovered Cambridge Analytica's improper actions. In the event that the controller or processor fails to follow the directives and therefore does not communicate the data breach, they could face heavy fines that could touch 20 million euros or 4% of the company's global turnover for any intentional or negligent violation of the GDPR.

[77] *Id.*
[78] *Id.*

Obviously, these numbers represent the extreme cases that generally apply when there are violations of the cardinal principles such as the lack of consent for the processing of personal data or the violation of privacy by design (which, as we mentioned earlier, consists precisely in the possibility for the data subject to decide for which data to give consent). For violations deemed minor or for inconsistencies in data management or archiving, the fine amounts to 2% of the global turnover. The last aspect to deal with is that of the global impact that an all-encompassing and extensive regulation such as the GDPR has had. Following in the footsteps of its predecessor, the GDPR must be adopted by all companies that use and process the data of data subjects located in the European territory even if the controllers and processors are not located in the EU. This, in addition to the fact that the GDPR also includes IP addresses as personal data, makes the regulation a truly worldwide law. Said in different terms, if for example a business were to be located in the USA, but still operate in the EU, it must still be certain that there is compliance with the dictates of the GDPR. The latter requires that local representatives be appointed in the EU states where the business is carried out.

3.2 THE PRIVACY JUNGLE

Although, as analyzed in the previous paragraph, Europe has committed itself to drafting a stringent regulation in terms of personal data protection, it is not said that social media companies respect the terms and conditions of the laws in force. In the paper *The Privacy Jungle: On the Market for Data Protection in Social Networks*[79], two scholars from the University of Cambridge, Joseph Bonneau and Soren Preibusch, set out to analyze the social media sector to verify whether all companies are respectful of the dictates imposed by the European Community and to better understand the shape of this industry. The results will be, that contrary to what was postulated, the market would not represent a true oligopoly since evidence supporting strong competition has been highlighted, especially among new users. But, above all, the two scholars have created a new economic model, the privacy communication game[80], according to which the economically rational choice for a site operator would be to make privacy control available, however making its interface difficult to access for discourage fundamentalists users.

[79] Bonneau, J., Preibusch, S. (2010). The Privacy Jungle: On the Market for Data Protection in Social Networks. In: Moore, T., Pym, D., Ioannidis, C. (eds) Economics of Information Security and Privacy. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-6967-5_8

[80] The two researchers talk about game in the sense of strategy applied by social media companies when they are faced with privacy concerns. However, it is important to underline that this "game" does not fall within the canonical definition identifiable in any game theory or industrial organization manual.

- **Survey Methodology and Data Collection**

The two scholars selected 45 social networking sites that were representative of different categories of social media. In particular, both general-purpose sites and niche sites are included in the research in such a way as to take into consideration a large statistical sample of users with different demographic and personal characteristics. General purposes sites are defined as those social networking services where anyone can register and participate freely. Generally, on these sites, of which an example are Facebook, Twitter, MySpace, users tend to present themselves with their real-world identity. The primary objective of this type of social network is to encourage interaction between users through other profile pages, a goal which very often coincides with the need of the users themselves who have an interest in transporting their relationships into a virtual space, favoring continuous interaction with others. Sites whose primary objective is to generate and share content (such as Youtube and Flickr) were excluded from this selection. Another omission concerns sites that are not available in English or accessible in Europe. From here comes a selection of 29 websites with a minimum of 500,000 users each.
On the other hand, niche sites are defined as all those sites that can be considered as a subset of general-purpose sites and that are characterized by the presence of specialized communities and characterized by a well-defined interest and/or need that must be satisfied through interaction on the social media in question.
We can distinguish the niche sites in subcategories based on the domain of interest of their users, from here we have:

- **Business-networking sites** = social networks specialized in job search and professional relationships. Users usually share information about their professional career and information related to professional and academic enrichment paths. They represent the digitalization of the job market by offering users the ability to interact with recruiters and access job positions more easily. Examples are LinkedIn, XING and Viadeo.
- **Media recommendation sites** = these sites encourage the sharing of multimedia content by creating communities of users with similar tastes and personal characteristics. They are particularly known and used by users who have a specific passion such as cinema, music or art and are used to generate exchanges between users of the same community around a common theme. These include Last.fm, Flickster and Buzznet.

- **Reunion sites** = they are proposed as sites to maintain social relationships between people looking for old acquaintances. In reality, they serve more as search engines between people than as promoters of online interactions, since very often these then move into real life. In recent years they have taken on an extremist note, becoming meeting places for political extremists.
- **Activity-focused sites** = are based on facilitating users to perform a specific activity. Very often they are a meeting point for gamers or students on international mobility. All microblogs are also included in this category.
- **Privacy-specific sites** = those sites that have privacy-specific features. They therefore allow information to be shared in total anonymity or through strong control of what is shared.

In the next page, a table (Fig.9) representing all the sites involved in the survey divided by traffic rank, millions of users, country (i.e., the country where the social network was developed and where the headquarters are located) and category based on the distinction stated earlier.

Site	Traffic Rank	Users (M)	Country	Category
Windows Live Spaces	4	120	USA	General-purpose
Facebook	5	175	USA	General-purpose
MySpace	7	250	USA	General-purpose
hi5	17	60	USA	General-purpose
SkyRock	43	13	France	General-purpose
Friendster	45	95	USA	General-purpose
NetLog	71	35	Belgium	General-purpose
Tagged	75	70	USA	General-purpose
Orkut	83	67	USA	General-purpose
LiveJournal	85	18	Russia	General-purpose
Bebo	119	40	USA	General-purpose
PerfSpot	124	20	USA	General-purpose
meinVZ	156	12	Germany	General-purpose
Multiply	161	12	USA	General-purpose
Badoo	168	19	UK	General-purpose
Sonico	183	33	Argentina	General-purpose
Ning	187	1	USA	General-purpose
CyWorld	315	20	South Korea	General-purpose
Xanga	346	40	USA	General-purpose
MyYearbook	406	15	USA	General-purpose
BlackPlanet	1021	18	USA	General-purpose
Plaxo	1486	20	USA	General-purpose
MocoSpace	2582	2	USA	General-purpose
Hyves	4166	8	Netherlands	General-purpose
Impulse	4782	1	Bulgaria	General-purpose
Yonja	5142	4	USA	General-purpose
Bahu	9977	1	France	General-purpose
Nexopia	12109	1	Canada	General-purpose
Eons	17872	1	USA	General-purpose
LinkedIn	149	35	USA	Business-networking
Imeem	186	30	USA	Media recommendation
Last.fm	317	21	USA	Media recommendation
Twitter	338	6	USA	Micro-blogging
Classmates.com	519	40	USA	Reunion
Gaia Online	628	7	USA	Gaming
MyLife	796	58	USA	Reunion
BuzzNet	954	10	USA	Media recommendation
Flixster	975	62	USA	Media recommendation
XING	1023	7	Germany	Business-networking
Viadeo	3280	7	France	Business-networking
Habbo	3349	124	Finland	Gaming
CouchSurfing	4326	1	USA	Travel
Experience Project	8878	2	USA	Privacy-specific
Kaioo	120679	n/a	Germany	Privacy-specific
Imbee	248170	n/a	USA	Privacy-specific

Table 1: Evaluated Social Networks, $N = 45$. User count in millions, rounded.

Figure 9

The evaluation method of all these sites has been standardized in such a way as to ensure homogeneity in the analysis of the data which are all contextual to the drafting period of the paper. Still, it is important to underline how the dynamism of the social media world is such as to make this environment particularly changeable, which is why only one time window has been considered. The analysis process can be divided into three steps: the first one has to do with the collection of general information regarding the site such as the date of entry on the web, the catchment area and web traffic. Subsequently, the scholars registered on the various social networks, recording the amount of personal information requested by each platform (it is important to underline that a standard persona had been created in such a way as to guarantee the homogeneity of the information entered), as well as the extent of the privacy control and the privacy policies offered by each site. Finally, these data were combined to analyze the formal privacy policies offered by each social network on the basis of some fixed factors including accessibility, length, role of third-party companies in data collection and existence of infrastructures to report abuse of data and help pages. The most interesting data reported by the research mainly concern the multilingualism of the sites, which was found to be significantly high with an average value of 9.1 languages offered to the user per site, and the competition in force between the various social media. According to the research, there would be significant competition whereby any single site would be competing against another social network in at least one market. A dynamic that becomes even more common and peculiar in Europe where data have shown that in most countries domestic platforms are strongly competing against international ones trying to avoid acquisition.

Other interesting developments from data analysis concern the business model adopted by social networks which would be based largely on profits deriving from the sale of advertising space and the presence of differentiated membership plans[81]. The promotion methods, on the other hand, would be mostly focused on maximizing the conversion rate among non-users through marketing strategies mainly focused on promoting social interactions and exploiting the network effects, typical of social media and already mentioned in the previous paragraphs of this thesis. Only 7 out of 29 sites would exploit their privacy controls features for promotional purposes. However, no site ever explicitly refers to the privacy policy making it clear that privacy is never used as the main argument to convince a user to subscribe to the site. Before moving on to analyzing privacy policies and how they are presented to users, a few words about the data collected during sign-up. It was reported that there was more data required by individual sites than what was actually needed to create an account. For example, 20 sites reported gender as mandatory, while 24 required a complete date of birth with only 6 of these sites allowing this data to be obscured in the profile. An

[81] Much more common on niche sites than on general-purposes sites.

absolutely unnecessary amount of data as the basis is not verifiable and implements, at most, a personalization of the user's profile. However, this data would instead provide much-needed information to be able to carry out profiling based on demographic factors.

- **Privacy Policies and Privacy Control Evaluation**

By privacy control we mean the set of options available to the user for the management of their data: i.e., to whom these are provided, how they are presented on the web and to whom and by what means they are accessible. In most cases, the most present option in terms of privacy control would concern profile visibility. The available options would concern accessibility via search engine[82], to site users only or "friends only". However, this would only represent a mere privacy strategy since membership of each site is simple and free, so the extrapolation of a user's data is the same if they decide to open their profile to the social network community. Instead, it represents a valid strategy to attract new users for social media companies that encourage the creation of accounts[83] to be able to view the profiles of acquaintances or friends. In addition to this problem, there would also be a too complex user interface which would therefore result in a limitation of the users' ability to effectively use the available privacy controls. In fact, most of the sites presented their features in a too complicated way despite scientific studies according to which offering users too much information in a disordered and hyper-configured way would reduce their ability to use them[84]. Coming to the analysis of privacy policies, these represent a legal contract between the social media company and the user and therefore, in order to be considered valid, they must be linguistically and technically accessible. More factors are therefore used in the exhaustive analysis of a privacy policy including:

1. **Technical Accessibility** = the privacy policy must be accessible through various search engines and devices. It must allow you to zoom in and read the text correctly, in some cases it is preferable to offer the possibility of printing the policy or being able to save it on the device.
2. **Length** = the policy must be of a length suitable for reading and correct understanding by the user.
3. **Legal issue** = as binding contracts, they should provide some basic contractual information.

[82] Which would be the equivalent of "make visible to everyone".
[83] Even fake ones very often, since, as we said before, so much data is not verifiable.
[84] Tony Vila, Rachel Greenstadt, and David Molnar. Why We Can't Be Bothered to Read Privacy Policies: Models of Privacy Economics as a Lemons Market. In ICEC '03: Proceedings of the 5th International Conference on Electronic commerce, pages 403–407, New York, NY, USA, 2003. ACM.

4. **Data claims** = the privacy policy should specify what data will be recorded, by whom it will be recorded, where it will be sent and what use will be made of that data. Consent to the privacy policy should then be different from consent to the processing of personal data by third-party companies.

Below, a table (Fig.10) representing the results of the evaluation of privacy policies.

site	PP present	PP new window	PP requires JavaScript	P3P full	P3P compact	PP dated	PP word count	PP mobileOK	PP zoomable	PP durable Url	PP printable	PP savable	PP textually structured	PP contains operator email address	PP contains operator postal address	PP contains seal	PP external dispute resolution	PP Safe Harbor participant	PP specifies national laws	PP specifies data locations	PP specifies data retention period	PP IP address collected	PP browser data collected	PP external data collected	PP shares with third parties	PP data anonymised for third parties	PP shares with search engines	PP shares with law enforcement	PP has third-party advertisers	PP user can delete data	PP user notified of changes	PP changes take effect delayed	TC minimum age
Badoo	y	n	n	y	n	n	1713	100	y	y	y	y	y	n	y	n	n	n	n	n	n	y	y	y	y	y		y		y	y		18
Bahu	y	n	n	n	n	n	266	91	y	y	y	y	y	y	n	n	n	n	n	n	n				n					y	n	n	13
Bebo	y	n	n	n	n	y	2842	42	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y		y	y	y	y	n	13
BlackPlanet	y	y	n	n	n	y	2888	100	y	y	y	y	y	y	y	n	n	n	y	n	n	y	y	y	y	n		y	y	u	y	n	14
BuzzNet	y	n	n	n	n	y	1781	86	n	y	y	n	y	y	y	n	n	n	n	y	n	y	y		y	y	y	y	y	y	n	n	13
Classmates.com	y	y	y	y	y	y	4934	48	y	y	y	y	y	y	y	y	y	n	y	y	n	y	y	y	y	n		y	y	u	y	y	13
CouchSurfing	y	n	n	n	n	n	1211	53	y	y	y	y	y	n	n	n	n	n	n	n	n	y		y	y	n				y	y	n	18
CyWorld	y	y	n	n	n	y	1870	54	y	y	y	n	y	y	n	n	n	n	n	y	n	y	y		y	y		y	y	u	n	y	13
Eons	y	y	n	n	y	y	1814	80	y	y	y	y	y	n	y	n	n	n	n	n	n	y	y	y	y	y		y	y		y	n	13
Experience Project	y	n	n	n	n	y	1502	91	y	y	y	y	y	y	n	n	n	n	n	n	n	y	y		y	n		y		y	y	n	13
Facebook	y	y	n	n	u	y	3765	56	y	y	y	y	y	n	y	y	y	n	y	y	n	y	y	y	y	n	y	y	y	y	y	y	
Flixster	y	n	n	y	n	y	2254	65	y	y	y	y	y	n	y	n	n	n	n	y	n	y	y		y	n		y	y	y	y	n	13
Friendster	y	y	y	n	n	y	1973	83	y	y	y	y	y	y	y	n	n	y	y	y	n	y	y		y	y		y	y		n	n	
Gaia Online	y	n	n	n	n	y	2249	63	y	y	y	y	y	y	y	n	n	n	n	y	n	y	y		y	y		y	y	u	y	n	13
Habbo	y	y	n	n	y	y	4166	47	n	y	y	y	y	y	y	n	n	n	y	y	n	y	y	y	y	n		y	y	y	n	n	13
hi5	y	n	n	n	n	y	2193	87	y	y	y	y	y	y	y	n	n	n	n	y	n	y	y		y	n		y	y	y	y	n	
Hyves	y	y	n	u	n	y	1706	38	y	y	y	y	y	n	n	n	n	n	y	y	n	y	y		y	n		y			n	n	0
Imbee	y	n	n	n	n	y	2240		y	y	y	y	y	y	y	n	n	n	y	n	n	y						y		y	n	n	
Imeem	y	n	n	n	n	y	1887	46	y	y	y	y	y	y	y	n	n	n	y	y	n	y	y		y	y		y	y	y	y	n	13
Impulse	n			n	n																												13
Kaioo	y	n	y	n	n	n	1418	57	y	n	y	n	y	y	n	n	n	n	y	n	n				n			y	n	u	n	n	14
Last.fm	y	y	n	n	n	y	4374	37	y	y	y	y	y	y	y	n	n	n	y	y	n	y	y	n	y	n		y	y		n	n	13
LinkedIn	y	y	n	n	y	y	4957	58	y	y	y	y	y	y	y	y	y	y	y	y	n	y	y			y	y	y	y	u	y	n	18
LiveJournal	y	n	n	n	n	y	2655	69	y	y	y	y	y	y	n	n	n	n	y	n	n	y	y	y	y	n		y	y	u	y		13
meinVZ	y	y	n	n	n	y	8455	52	y	y	y	y	y	y	y	n	n	n	y	y	y	y	y		n			y	y	y			18
MocoSpace	y	n	n	n	n	n	1344	71	y	y	y	y	y	y	n	n	n	n	n	n	n	y	y		y	y		y	y	y	y	n	13
Multiply	y	n	n	n	n	n	2142	65	y	y	y	y	y	n	n	n	n	n	y	n	n	y	y		y	y		y	y	y	n	n	13
MyLife	y	n	n	y	y	n	4083	57	y	y	y	y	y	n	y	y	y	n	n	n	n	y	y	y	y	n	y	y	y	y	y	n	13
MySpace	y	y	n	n	n	y	2738	45	y	y	y	n	y	y	y	n	n	n	n	y	n	y	y		y	n		y	y		n	n	13
MyYearbook	y	n	n	n	n	y	955	57	y	y	y	y	y	n	y	n	n	n	n	n	n	y	y	y	y	n		y	y			n	13
NetLog	y	y	n	n	n	n	311	94	y	y	y	y	n	y	y	n	n	n	y	y	n							y		u			
Nexopia	y	n	n	n	n	y	2752	39	n	y	y	y	y	y	y	n	n	n	n	y	n	y	y		y	y		y	n	u	y	n	13
Ning	y	n	n	n	u	y	4135	79	y	y	y	y	y	y	y	n	n	n	y	y	n	y	y	y	n			y	n	u	n	n	13
Orkut	y	n	n	u	n	y	3073	80	y	y	y	y	y	n	y	n	n	y	y	y	n	y	y	y	y	y		y	y	y	y	n	
PerfSpot	y	n	n	n	n	y	2108	20	y	y	y	y	y	y	y	n	n	n	y	n	n	y	y		y	n		y	y	n	n	n	13
Plaxo	y	n	n	n	n	y	4271	51	y	y	y	y	y	y	y	y	y	y	n	n	y	y	y		y	y		y		y	y	y	13
SkyRock	n	n	n	n	y	n	641	69	y	y	n	y	y	n	y	n	n	n	y	y	n	y	y					y		y			
Sonico	y	n	n	n	n	n	923	73	y	y	y	y	y	y	n	n	n	n	n	n	n				n					u			
Tagged	y	y	y	n	n	y	2799	68	y	y	y	y	y	y	y	n	n	n	y	y	n	y	y		y	n		y	y	u	n	n	13
Twitter	y	n	n	n	n	y	1535	67	y	y	y	y	y	y	n	n	n	n	y	y	n	y	y		y	n		y		y	y	n	13
Viadeo	y	n	n	y	y	n	2848	18	n	y	y	y	y	n	y	n	n	n	y	n	n	y	y		n					y	n	n	18
Windows Live Spaces	y	y	n	n	u	y	4361		y	y	y	y	y	n	y	y	n	y	y	y	n	y	y	y	y	y		y	y		y	n	
Xanga	y	n	n	n	n	n	4948	55	y	y	y	y	y	n	n	n	n	n	n	y	n	y	y		y	y	y	y	y	u	y	n	13
XING	y	n	n	n	n	y	3237	58	y	y	y	y	y	n	n	n	n	n	y	n	n	y	y		n		y				y	n	17
Yonja	y	n	n	n	n	n	1557	56	y	y	y	y	y	n	n	n	n	n	n	n	n	y	y		n			y	y	u	y	y	18
Impulse (T&C)	u	n	n	n	n	n	32	67	y	y	y	y	y	n	n	n	n	n	n	n	n				n			y			n	n	13

Figure 10 where y stands for "yes", n stands for "no" and u is "implemented with errors"

Wanting to analyze which factors are related to good practices in terms of privacy, the researchers decided to use the data available to them by determining scores for each site involved in the analysis. The global privacy score would then be divided into three subscores, namely:

- **data collection score**: inherent to data collection practices.
- **privacy control interface:** relating to the usability of the privacy controls interface.
- **privacy policy:** overall vote on the privacy policy based on the factors listed above.

Below (Fig.11), the formula used for the calculations.

$$\text{Privacy Score} = \frac{\frac{\text{PCS}-\min(\text{PCS})}{\max(\text{PCS})-\min(\text{PCS})} + \frac{\text{PPS}-\min(\text{PPS})}{\max(\text{PPS})-\min(\text{PPS})} + 1 - \frac{\text{DCS}-\min(\text{DCS})}{\max(\text{DCS})-\min(\text{DCS})}}{3}$$

Figure 11

The privacy score aims to aggregate the three subscores and is calculated just like the arithmetic mean between the three.

The data collection subscore (DCS) is calculated as the sum of the number of data items requested and required by each site. It is calculated by assigning 1 point for each required data and 0.5 points for each requested data. Items that require verification or validation receive 2 points instead.

The privacy control subscore (PCS) would instead represent the number of features implemented by each site that would allow the user to control the privacy of the profile. Again, 1 point is awarded for each feature in the following table (Fig.12).

feature	scoring	adjustments
data security		
full TLS during login	+2.0pt	−1.0pt POST only
can logout from site	+1.0pt	
privacy configurability		
Friends-only visibility available	+1.0pt	+1.0pt if default setting
Network-only visibility available	+1.0pt	+1.0pt if default setting
Profile line-item ACL available	+1.0pt	+0.1pt each item up to a maximum of +3.0pts
Photo, commenting, messaging ACL	+1.0pt each	
List-based ACL	+1.0pt	
Audience view	+1.0pt	
Search view	+1.0pt	
Pre-set privacy combinations	+1.0pt	
Email settings	+1.0pt	
privacy support by site operator		
Privacy settings Help	+1.0pt	
Block User Button	+1.0pt	
Report User Button	+1.0pt	
Abuse Reporting	+1.0pt	+1.0pt telephone
Privacy Tips	+1.0pt	
Safety Tips	+1.0pt	
Parent Tips	+1.0pt	

Figure 12

The privacy policy subscore (PPS) is calculated on the basis of accessibility, availability during the sign-up process and the amount of information expected. The following table (Fig.13) explains the scoring in detail.

feature	scoring	adjustments
accessibility		
PP acknowledgement checkbox	+1.0pt	
PP link presented during signup	+1.0pt	−0.5pt requires JavaScript and −0.25pt pop-up window
T&C link presented during signup	+1.0pt	−0.5pt requires JavaScript and −0.25pt pop-up window
number of links available to PP	+0.5pt per link	up to a maximum of +2.0pts
number of links available to T&C	+0.5pt per link	up to a maximum of +2.0pts
usage		
PP exists	+1.0pt	−1.0pt requires JavaScript
PP dated	+1.0pt	
mobileOK percentage score	+0.00.. + 1.00pt	
PP bookmarkable	+1.0pt	
PP printable	+1.0pt	
PP savable	+1.0pt	
PP textually structured	+1.0pt	
privacy statements		
Can delete personal information	+1.0pt	−0.5pt partial deletion only
National laws obeyed specified	+1.0pt	
Privacy seal	+1.0pt	
Collection of data from external sources	−1.0pt	
Sharing data with third parties	−1.0pt	−2.0pt not anonymised
contact details		
Contains operator email address	+1.0pt	
Contains operator postal address	+1.0pt	
privacy policy mutability		
Users notified of changes to PP	+1.0pt	
Delay period before changes effective	+1.0pt	
P3P deployment		
Full P3P policy	+1.0pt	−0.5pt if not correct
Compact P3P policy	+1.0pt	−0.5pt if not correct

Figure 13

Finally, a functionality score was also determined which represents the amount of additional and unnecessary features implemented by each site. 1 point is awarded for each feature and 2 points for those managed by third parties (Fig.14).

feature	scoring
meta-functionality	
Third-party applications	+2.0pt
interactivity	
Profile commenting	+1.0pt
Sending messages to other users	+1.0pt
Photo uploading	+1.0pt
Photo tagging	+1.0pt
Event streaming	+1.0pt
connectivity	
Data export protocol	+1.0pt
OpenID	+1.0pt
Linkable “profile badges”	+1.0pt

Figure 14

Having therefore defined how the scores are calculated, the attribution table for each site involved in the survey is shown below (Fig.15).

Site	1 – Data Collection Score	Privacy Control Score	Privacy Policy Score	Privacy Score	Function-ality Score
Badoo	.33	.07	.33	**.23**	.40
Bahu	.24	.22	.43	**.35**	.50
Bebo	.62	.44	.57	**.70**	.60
BlackPlanet	.29	.26	.54	**.46**	.50
BuzzNet	.29	.22	.43	**.37**	.60
Classmates.com	.33	.22	.63	**.51**	.30
CouchSurfing	.14	.30	.26	**.26**	.30
CyWorld	.14	.47	.50	**.51**	.50
Eons	.24	.36	.48	**.46**	.50
Experience Project	.81	.19	.30	**.44**	.30
Facebook	.10	.61	.41	**.53**	.90
Flixster	.33	.26	.48	**.44**	.40
Friendster	.29	.30	.48	**.44**	.60
Gaia Online	.81	.44	.46	**.69**	.30
Habbo	.81	.37	.48	**.66**	.50
hi5	.43	.32	.43	**.48**	.70
Hyves	.29	.41	.41	**.47**	.70
Imbee	.05	.37	.57	**.46**	.30
Imeem	.71	.15	.57	**.55**	.50
Impulse	.43	.34	.13	**.30**	.30
Kaioo	.57	.15	.46	**.43**	.20
Last.fm	1.00	.22	.48	**.64**	.40
LinkedIn	.52	.39	.67	**.70**	.50
LiveJournal	.48	.60	.37	**.62**	.50
meinVZ	.38	.41	.65	**.65**	.40
MocoSpace	.52	.30	.43	**.49**	.30
Multiply	.05	.36	.39	**.34**	.40
MyLife	.29	.07	.43	**.28**	.30
MySpace	.29	.41	.43	**.48**	.80
MyYearbook	.24	.44	.17	**.33**	.70
NetLog	.52	.30	.35	**.44**	.60
Nexopia	.33	.22	.46	**.40**	.30
Ning	.52	.41	.48	**.59**	.70
Orkut	.43	.35	.46	**.51**	.70
PerfSpot	.19	.63	.48	**.61**	.60
Plaxo	.29	.44	.57	**.58**	.40
SkyRock	.38	.11	.39	**.31**	.40
Sonico	.00	.33	.37	**.30**	.30
Tagged	.24	.22	.35	**.30**	.60
Twitter	.81	.26	.30	**.49**	.10
Viadeo	.43	.15	.50	**.41**	.20
Windows Live Spaces	.33	.47	.50	**.58**	.80
Xanga	.76	.48	.37	**.65**	.50
XING	.24	.37	.57	**.52**	.30
Yonja	.57	.33	.37	**.49**	.40

Figure 15

Through the analysis of this data, a positive correlation between the age of a site and its privacy score emerged. Typically, a site that has been around longer has a more detailed privacy policy as a reaction to a policy engineering process.
At the same time, there is a positive relationship between the size of a site[85] and the privacy score and this is mainly determined by the fact that a large company can devote more resources to structuring a department management of these tasks.
The differentiation in privacy choices is the result of the lack of universal rules about privacy in social networking. This is why a model has been proposed, the privacy communication game, which can explain how and why certain choices are made by companies from a strategic point of view.

- **The Privacy Communication Game**

Before introducing the model, it must be specified that within the same model there are different types of users who have different privacy concerns. These can be divided into three categories: *marginally concerned, pragmatic majority, privacy fundamentalists*, a taxonomy attributable to Westin[86]. The largest group[87] would be that of the pragmatic majority which would be interested in issues concerning the respect of online privacy, but which easily tends to bypass this interest if they are offered an attractive service or a monetary reward[88].
A successful site, therefore, will play a game of minimizing the fundamentalists' concern while also minimizing the awareness of privacy for the marginally concerned. The fundamentalists are those who extensively care about their privacy and the use that is made of their personal data, therefore they represent the sentinels of the group who pay attention to the purposes and activities of each social network. If, for example, a social media operator was to operate in an unlawful way in terms of personal data processing, the fundamentalists would alert the marginally concerned[89] and both groups would abandon the social network. The range of action of a social media operator would therefore be ⟨communicate, hide⟩. All users (both fundamentalists and marginally concerned) can choose between ⟨sign up, cancel⟩, while only fundamentalists have an additional choice between

[85] In terms of user base and geographical operations.
[86] Mark S. Ackerman, Lorrie Faith Cranor, and Joseph Reagle. Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences. In EC '99: Proceedings of the 1st ACM conference on Electronic commerce, pages 1–8, New York, NY, USA, 1999. ACM.
[87] In terms of number of users.
[88] Sarah Spiekermann, Jens Grossklags, and Bettina Berendt. E-privacy in 2nd Generation E-commerce: Privacy Preferences Versus Actual Behavior. In EC '01: Proceedings of the 3rd ACM conference on Electronic Commerce, pages 38–47, New York, NY, USA, 2001. ACM.
[89] who must be imagined as the type of users who are interested in the topic but have no interest to search for information to be sure that their privacy is respected.

⟨complain, silence⟩ in case there is a breach of privacy. Since the operator adopts different strategies on the basis of the two groups of users, he can maximize the outcome by dividing the two groups by the signals received on the basis of privacy preferences and then discriminate them by adopting user-based strategies. The underlying concept is similar to the price discrimination adopted by companies. In addition, this model excludes external actors such as journalists who could influence public opinion more[90].

The main objective of social media companies when faced with the marginally concerned is not only to encourage sign-up, but also the disclosure of information. The operator therefore has an interest in creating an environment where everyone can feel free to disclose their data which, studies have shown, non-fundamentalists are more inclined to do when there is only the slightest reference to privacy[91]. This phenomenon is known as *privacy salience* and indicates that providing strong privacy assurance may actually make users less inclined to disclose their information online. Due to the effects of privacy salience, even the promotion of positive privacy practices can reduce willingness to disclose personal information, which would explain why many social media companies do not use the issue of privacy as a theme for promoting their platform.

On the other hand, the fundamentalists represent only a small portion of the general market since research has shown that more privacy-inclined people are less willing to subscribe to a social media[92]. Reason why a site should, in a certain way, "discourage" privacy fundamentalists, but without giving them reasons to complain about the service offered. Indeed, privacy fundamentalists would bring indirect costs to a social network site such as the opportunity cost deriving from the fact that fundamentalists are less inclined to disclose information[93] and the increase in privacy salience of non-fundamentalists. The indirect costs should then be added to the direct costs deriving from offering a free service without making any profit. This therefore explains why many social networks do not implement additional security tools by offering users the bare minimum. This strategy would not alter the privacy fundamentalists who could not complain since all the regulations would be respected, but it would also offer them a deterrent from joining the social network. In addition to this strategy, a successful social networking site should also attempt to reduce criticism by allowing free and optional access to the full privacy policy.

[90] McCombs and D.L. Shaw. The Agenda-Setting Function Of Mass Media. Public Opinion Quarterly, 36(2):176–187, 1972.

[91] George Loewenstein. Keynote Speech: Searching for Privacy in all the Wrong Places: A Behavioral Economics Perspective on Individual Concern for Privacy. WEIS 07: The Seventh Workshop on the Economics of Information Security, June 2007.

[92] Alessandro Acquisti and Ralph Gross. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In Privacy Enhancing Technologies – LNCS 4258, pages 36–58. Springer Berlin / Heildelberg, 2006.

[93] Cliff A.C. Lampe, Nicole Ellison, and Charles Steinfield. A Familiar Face(book): Profile Elements as Signals in an Online Social Network. In CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems, pages 435–444, New York, NY, USA, 2007. ACM.

Combining the two strategies stated above and based on different user groups, we can conclude that the best mixed strategy to apply for this privacy discrimination model is the one that evolves according to the evolution of the user base. It can be expected that the marginally concerned will form the early adopters base of our innovation cycle, therefore a social networking website should start by implementing the privacy features necessary to be able to operate according to the law in such a way as to minimize privacy salience and maximize growth in the short term. Once it has moved to a more stable phase of its business cycle, in which we expect the entry of new categories of users including privacy fundamentalists, the social network site should start implementing additional personal data control mechanisms in in such a way as to avoid the complain of the fundamentalists. We can conclude that the privacy market on social media can be compared to a lemons market[94], i.e., a market where there is information asymmetry between the offeror (in our case, the social media companies) and the buyer (in our case, the user). Since users find it more difficult to assess a site's privacy, they have less incentive to provide good features leaving the market in the hands of the lemons. This would therefore explain why privacy policies would report huge usability problems. Since this paper dates back to 2010, I checked if these results were still realistic today given the great changeability of the social media market. A 2020 paper, *The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services*[95], actually confirmed this theoretical modeling by highlighting how many users make a very approximate reading of privacy policies or, even, skipping them by clicking immediately on the click box for registration. In recent years, a *privacy paradox* has been generated according to which many users would actually be interested in the privacy mechanisms of social network sites while then, in reality, they would not act accordingly, paying little or no attention when using the social media.

[94] Id. *supra note* 79.
[95] Obar, J., & Oeldorf-Hirsch, A. (n.d.). The biggest lie on the internet: Ignoring the privacy policies and terms of service of social networking services. Taylor & Francis online. https://www.tandfonline.com/doi/full/10.1080/1369118X.2018.1486870

CONCLUSION

In the course of this thesis various points of interest have been touched upon which I would like to summarize before reaching the final conclusion.

We started from the presentation and analysis of the Cambridge Analytica case study. The case in question is peculiar, first of all because it is one of the few that can be considered concluded since the legal deliberations have reached the last stages of appeal and, secondly, because in addition to being the first uncovered case of abuse of computer data for activity of an economic nature, it is also the one of which we know all the details. Starting from this case study was therefore essential to put readers in front of what could really happen (and has really happened) in the event that our data ends up in the wrong hands. Companies like Cambridge Analytica could take over our lives and unknowingly influence our choices through hyper-profiling activities.

We then moved on to the analysis of the reference industry, that of social media. It was underlined how in the most common sense the social media market was born as an oligopoly, a few companies competing for the global market. Meaning that, however, is not reflected in reality. Social media companies, differently from what one might think, have no incentive to cooperate with each other and are characterized by a strong level of domestic competition, albeit at an international level, however, there are no major competitors. After this brief expenditure, Meta and its merger and acquisitions strategy, which began with purely expansionary and technological innovation purposes, were analyzed: at the beginning, Meta mostly acquired start-ups that served as integration to the services already offered by the company for then move on to a real operation of engulfing its competitors which first occurred with the acquisition of Instagram. Hence, a doubt: does centralizing the data of a multitude of users in the hands of a single organization, in this case Meta, represent a risk for the protection of personal data?

The same question that governments around the world have tried to answer through legislative actions that trace a clear path for the range of action of these companies. Thus, the General Protection Data Regulation was examined, launched by the European Union with the intention of putting a stop to the inconsiderate use of data by European citizens with a major innovation, i.e., the introduction of a specific so these same rules apply to companies that process data of anyone transiting through Europe, creating a sort of protected area. However, this is not enough since if a European citizen were to move to the USA, even for a very short period, he would no longer be protected by this regulation. From here we have therefore moved on to what we can do individually to prevent our data from being exploited in an inconsiderate way and this has led to the in-depth analysis of privacy policies, i.e., those policies that we all subscribe to by subscribing to a social network and of which, generally, we are not aware of. And also the strategy of social media

companies by which they do not offer user-friendly interfaces and apply a specific business strategy as highlighted through the privacy communication game.

The general point of this whole process is that however hyperdeveloped it may be by now, the social media industry lacks an exhaustive regulation that can eliminate any shadow cone to the detriment of the consumer. The game that is going to be played in this playing field is not on equal terms and strongly suffers from information asymmetry. On the one hand, the user is not perfectly informed about the use of his data due to excessively long and difficult to understand privacy policies, on the other he doesn't even have the desire to get informed properly and in order to be able to use the service for free he decides to turn a blind eye. On the other hand, we have companies like Cambridge Analytica that buy packets of data from social networks that do not supervise and do not pay attention to who they are going to sell the data for the sake of selling them and exploit them without specifying the final use. Finally, we have a company, Meta, which is incorporating its competitors determining a risk not only in terms of antitrust, but also in terms of data management since any breach could be potentially fatal for the identity of millions of users. A monopoly, therefore, which has been making its way over the last few years and to which little attention is being paid or it is being considered a small risk. The hope is that of a better defined framework of the market contexts, in such a way as to be able to theorize more effectively the processes that are applied by individual companies, and of more stringent and detailed legislation, but above all in spirit that can see the collaboration between several nations and therefore favor international cooperation and a range of action in borderline cases that is not left to intentionality or to the specifics of a single legal system, but can meet a single rational process or at least of international scope in multiple jurisdictions.

BIBLIOGRAPHY

Amy Mitchell, Mark Jurkowitz, J. Baxter Oliphant, Elisa Shearer (2020, July 30). Demographics of Americans who get most of their political news from social media. Pew Research Center. Retrieved February 15, 2022 from https://www.pewresearch.org/journalism/2020/07/30/demographics-of-americans-who-get-most-of-their-political-news-from-social-media/

Bainbridge, S.M. (2020). Corporate Law. Foundation Press.

Bainbridge, S.M. (2020). Mergers and Acquisitions. In Corporate law (pp. 410–412). Book, Foundation Press.

BBC. (2016, September 13). Hillary Clinton 'kept pneumonia diagnosis from most of team'. BBC News. Retrieved February 19, 2023, from https://www.bbc.com/news/election-us-2016-37346293

BBC. (n.d.). EU referendum results. BBC News. Retrieved February 19, 2023, from https://www.bbc.co.uk/news/politics/eu_referendum/results

Breach of trust - law definition • sewell & kettle lawyers. Sewell & Kettle Lawyers. (2022, January 31). Retrieved February 20, 2023, from https://sklaw.au/dictionary/breach-of-trust/

Cadwalladr, C., & Jukes, P. (2018, June 16). leave. EU faces new questions over contacts with Russia. The Guardian. Retrieved February 19, 2023, from https://www.theguardian.com/uk-news/2018/jun/16/leave-eu-russia-arron-banks-andy-wigmore

Carole Cadwalladr, “I made Steve Bannon’s psychological warfare tool: meet the data war whistleblower”, Guardian (March 18, 2018) https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

Chen, B.X. (2018, March 21). Want to #deletefacebook? you can try. The New York Times. Retrieved February 20, 2023, from https://www.nytimes.com/2018/03/21/technology/personaltech/delete-facebook.html

Clinton, H. (2016, September 12). Thanks to everyone who's reached out with well wishes! I'm feeling fine and getting better. -H. Twitter. Retrieved February 19, 2023, from https://twitter.com/HillaryClinton/status/775435555601543168

Colander, David C. Microeconomics 7th ed. Page 288 McGraw-Hill 2008.

Council of Europe. (1950, September 3). European Convention for the protection of human rights and fundamental freedoms. Wikisource, the free online library. Retrieved April 11, 2023, from https://en.wikisource.org/wiki/European_Convention_for_the_Protection_of_Human_Rights_and_Fundamental_Freedoms

Council of Europe. (1981, January 28). Council of Europe Convention No. 108 on Data Protection. European Data Protection Supervisor. Retrieved April 11, 2023, from https://edps.europa.eu/data-protection/our-work/publications/legislation/council-europe-convention-no-108-data-protection_en

Disinformation and ‘fake news’: Interim report - digital, culture ... (n.d.). Retrieved February 19, 2023, from https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36308.htm

European Council. (2011). (rep.). Draft European Council decision . Retrieved February 19, 2023, from https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/118578.pdf#page=6.

European Union. (1995, October 24). Data Protection Directive 95/46/EC. EUR-Lex. Retrieved April 11, 2023, from https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A31995L0046

Geiger, A. (2021, April 9). Political polarization in the American public. Pew Research Center - US Politics & Politics. Retrieved February 19, 2023 from https://www.pewresearch.org/politics/2014/06/12/political-polarization-in-the-american-public/

Goldberg, L.R. (1993). The structure of phenotypic personality traits. American Psychologist, 48(1), 26–34. https://doi.org/10.1037/0003-066x.48.1.26

Hirschey, M. Managerial Economics. Rev. ed, page 451. Dryden 2000.

Investigation into payments made to better for the country and leave.EU. Electoral Commission. (n.d.). Retrieved February 19, 2023, from https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/our-enforcement-work/investigations/investigation-payments-made-better-country-and-leaveeu

Jones, B. (2022, October 26). An examination of the 2016 electorate, based on validated voters. Pew Research Center - U.S. Politics & Policy. Retrieved February 19, 2023, from https://www.pewresearch.org/politics/2018/08/09/an-examination-of-the-2016-electorate-based-on-validated-voters/

Kenton, W. (2022, December 24). European sovereign debt crisis: Eurozone crisis causes, impacts. Investopedia. Retrieved February 19, 2023, from https://www.investopedia.com/terms/e/european-sovereign-debt-crisis.asp

Kepios. (2023, January 1). Global Digital Report 2022. Kepios. Retrieved February 25, 2023, from https://kepios.com/reports

Kotler, P. (1989), “From mass marketing to mass customization”, Planning Review, SeptemberOctober, pp. 10-23 and 47.

Kristen Purcell, Lee Rainie (2014, December 8). Americans feel better informed thanks to the internet. Pew Research Center. Retrieved February 15, 2022 from https://www.pewresearch.org/internet/2014/12/08/better-informed/

Lewis, P., & Hilder, P. (2018, March 23). Leaked: Cambridge Analytica's blueprint for trump victory. The Guardian. Retrieved February 19, 2023, from https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analytics-blueprint-for-trump-victory

Matthew Rosenberg, Sheera Frenkel, “Facebook’s role in Data Misuse Sets Off Storms on Two Continents”, The New York Times. (March 18, 2018) https://www.nytimes.com/2018/03/18/us/cambridge-analytica-facebook-privacy-data.html

MirrorPolitics. (2016, May 17). David Cameron just claimed ISIS supports the EU referendum 'leave' campaign. mirror. Retrieved February 19, 2023, from https://www.mirror.co.uk/news/uk-news/isis-backs-brexit-david-cameron-7988647

OECD. (1999, January 5). Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data. OECD Legal Instruments. Retrieved April 11, 2023, from https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Osborne, Dale K. (August 1964). "The Role of Entry into Oligopoly Theory". The University of Chicago Press Journals. 72(4):396–402 – via JSTOR.

Politico: www.politico.com

Poropat, A. E. (2009). A meta-analysis of the five-factor model of personality and academic performance. Psychological Bulletin, 135(2), 322–338. https://doi.org/10.1037/a0014996

Posner, R.A. (2000). An affair of state the investigation, impeachment, and trial of President Clinton. Harvard University Press.

Privacy Guarantor. (n.d.). GDPR - Regulation 2016/679. GDPR - Regulation 2016/679 - Privacy Guarantor. https://www.garanteprivacy.it/regolamentoue

Reuters Staff (2018, August 7). Unicredit has stopped using Facebook for advertising: CEO. Reuters. Retrieved February 20, 2023, from https://www.reuters.com/article/us-facebook-unicredit/unicredit-has-stopped-using-facebook-for-advertising-ceo-idUSKBN1KS1N5

Samsel, Hamp; Svitek, P. (2018, March 20). Ted Cruz says Cambridge Analytica told his presidential campaign its data use was legal. The Texas Tribune. Retrieved February 18, 2023, from https://www.texastribune.org/2018/03/20/ted-cruz-campaign-cambridge-analytica/

Segall, L. (2018, March 21). CNN interview: Read Mark Zuckerberg's remarks. CNNMoney. Retrieved February 20, 2023, from https://money.cnn.com/2018/03/21/technology/mark-zuckerberg-cnn-interview-transcript/index.html

Sponsor-generated content: Ten inconvenient truths about the Clinton Foundation. (n.d.). Retrieved February 19, 2023, from https://www.politico.com/sponsor-content/2016/08/inconvenient-truths-about-clinton-foundation

Staff, the P.N.O., &; Nguyen, S. T. (2022, March 4). Premerger notification and the Merger Review process. Federal Trade Commission. Retrieved February 26, 2023, from https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/mergers/premerger-notification-merger-review-process

Stelter, B. (2018, March 25). Tweets. Twitter. Retrieved February 20, 2023, from https://twitter.com/brianstelter

Stigler, George J. (February 1964). "A Theory of Oligopoly". The University of Chicago Press Journals. 72(1):44–61 – via JSTOR.

TheKnow - our campaign. Our Campaign - Leave.eu. (n.d.). Retrieved February 19, 2023, from https://web.archive.org/web/20151013010834/http://leave.eu/en/our-campaign

U.S. Senate. (2018). (rep.). Putin's Asymmetric Assault On Democracy In Russia And Europe: Implications For U.S. National Security. Retrieved February 19, 2023, from https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

Weaver, M. (2018, April 17). Cambridge Analytica: Ex-director says firm pitched detailed strategy to leave.EU. The Guardian. Retrieved February 19, 2023, from https://www.theguardian.com/uk-news/2018/apr/17/cambridge-analytica-brittany-kaiser-leave-eu-brexit

Wikimedia Foundation (2022, December 9). *Paradox of Voting*. Wikipedia. Retrieved February 15, 2022 from https://en.wikipedia.org/wiki/Paradox_of_voting

Wikimedia Foundation. (2022, December 30). Nationwide opinion polling for the 2016 United States presidential election. Wikipedia. Retrieved February 19, 2023, from https://en.wikipedia.org/wiki/Nationwide_opinion_polling_for_the_2016_United_States_presidential_election