THE IMPLICATIONS OF TARGETTED ADVERTISING ON SOCIAL MEDIA PRIVACY POLICIES- THE CASE OF CAMBRIDGE ANALYTICA & FACEBOOK

Shreya Bhardwaj

Jindal school of Journalism and Communication, O.P. Jindal Global University

Student ID – 20177038

May 20, 2020

Abstract

Advertising is everywhere online, but we've gotten pretty good at ignoring it. To win back our attention, advertisers have adapted to our digital viewing habits by remembering what we read, what we buy, what we follow online, then using this information to sell us (products) they think we might like. While it may sound strange, this practice, called targeted advertising has become very common. In fact it has now become a part of our everyday life reaching an extent where even our political decisions are being influenced by the political advertising agencies using our own online information against us, in order to get us to vote for their candidate which eventually lead us to the Facebook- Cambridge Analytica data breach occurred in 2016 when millions of Facebook users' personal data was harvested without consent by a political consulting firm, Cambridge Analytica to be primarily used for political advertising. This data break is known to be the largest leak in the history of Facebook.

Keywords: Targeted advertising, Political advertising, Facebook, Cambridge Analytica

Contents

THE IMPLICATIONS OF TARGETTED ADVERTISING ON SOCIAL MEDIA PRIVACY POLICIES- THE CASE OF CAMBRIDGE ANALYTICA & FACEBOOK

According to a report 'Exploring the Big Data revolution' APIC, a trend that has grown exponentially in the past few years is Big Data. Big data, collection of data and technology that accesses, combines and reports all available data by filtering, correlating and reporting insights not attainable with past data technologies. Big data labels data processing beyond the human scale. In the past, databases tended to be limited as they were only expected to meet the demands of human users entering and retrieving data, but with the emergence ecommerce and internet search engines, database technology has been evolving to manage humans and computers and with the amount of information growing by 50% each year today, it is information technology that is capable of managing, processing and finding value.

Big data has been seemingly transforming many industries over time. One such industry that has seen the maximum impact in terms of profitability is advertising. The communication between the advertisers and consumers has changed drastically owing to the advancement in the big data technologies. Only with the help of big data, advertisers can now understand and optimize the demands of every single customer and convert them into prospective buyers.

However according to David W. Nickerson & Todd Rogers from Harvard university 2013, over the years, big data has also had quite an impact on political advertising in order to foresee future to maximize the political party's ability/probability of victory, as during a political campaign every aspect of the campaign is evaluated, like the number of votes an activity will generate along with the cost to perform a cost benefit analysis, campaigns need accurate predictions about the preferences of voters, their expected behaviors and their responses to the outreach which is only possible after analyzing large and detailed datasets. The improved

efficiency in political campaigns with the help of big data has led the political parties to engage in an arms race to leverage ever-growing volumes of data to create votes.

Online targeted advertising

Online advertising

Real-time mass media was born with national radio networks in the 1920s. As mass media gave rise to mass advertising, advertisers' campaigns became national. However, advertisements have merely been relevant to a small section of the viewership of any TV show, the audience of any radio programme or the readership of any newspaper. When the internet was introduced to the society, back in the 90s, it was never conceived as a means of advertising. It was merely created as a simple tool for the exchange of electronic mails and digital information. That is to say, the enormous impact that this simple tool would have in our lives was still unknown.

It was not long before the marketing pioneers started to see digital advertising as a big business. Growing users began to connect trying to search relevant information about their interests. For many advertising managers, this marked as a turning point in the history of online advertising.

Online advertising became one of the most effective ways for businesses of all sizes to expand their reach, find new customers, and diversify their revenue streams. Social networks such as Facebook, Twitter brought to the world a new form of consumer participation and a host of new possibilities to effectively reach all potential customers.

Targeted Advertising. It is a form of online advertising that focuses on the specific traits, interests, and preferences of a consumer. Advertisers discover this information

by TRACKING YOUR ACTIVITY on the Internet. Online advertising can be targeted to users most likely interested in a particular product or a service.

The consumer may benefit from ads targeted to their personal interests; saving the time it takes to find products and reducing irrelevant ads.

Behavioral targeting

Behavioural targeting is a type of marketing technique that has been used online for a number of years, as a way of allowing businesses to reach out to their target audience. The term itself is capable of suggesting that behavioural targeting can allow for entrepreneurs to match their sales tactics to the interests, socio-demographics and browsing behaviour shown by the prospective buyers. For instance, a person who has been comparing diaper brands on the internet may be easily persuadable to advertisements for diapers along with complementary products such as baby wipes, feeding bottles and baby monitors. Behavioural targeting gives markets and advertisers an opportunity to get far more clicks on their links, services or products then they normally would, as they are reaching out directly to a particular demographic or niche.

Advertising is a form of commercial communication with regard to an economic activity for promoting the commercialisation of any goods, services or any ideas or principles, institutions or initiatives, an essential element and motor of programming and economic development. It is undeniable that advertising takes a dual function i.e. informative and persuasive, it is through the advertisements that the consumer is aware of the characteristics of goods and services and makes business decisions, but also because the aim of advertising is to seduce, awake desires, induce needs and entice choices. The world of advertising receivers includes those to whom the advertising message is, directly or indirectly, addressed to and since the power of a brand depends primarily on its psychological effect on the public, no advertisers would want to spend their resources for trade promotion with consumers unrelated or

uninterested in the product or the offered service. That is why, behavioural targeting, in the voice of economic operators is quite essential to digital marketing and e-commerce.

Targeted advertising and its functions

Internet cookies

Cookies are small bits of text that are downloaded to your browser as you surf the web. Their purpose is to carry bits of useful information about your interaction with the website that sets them.

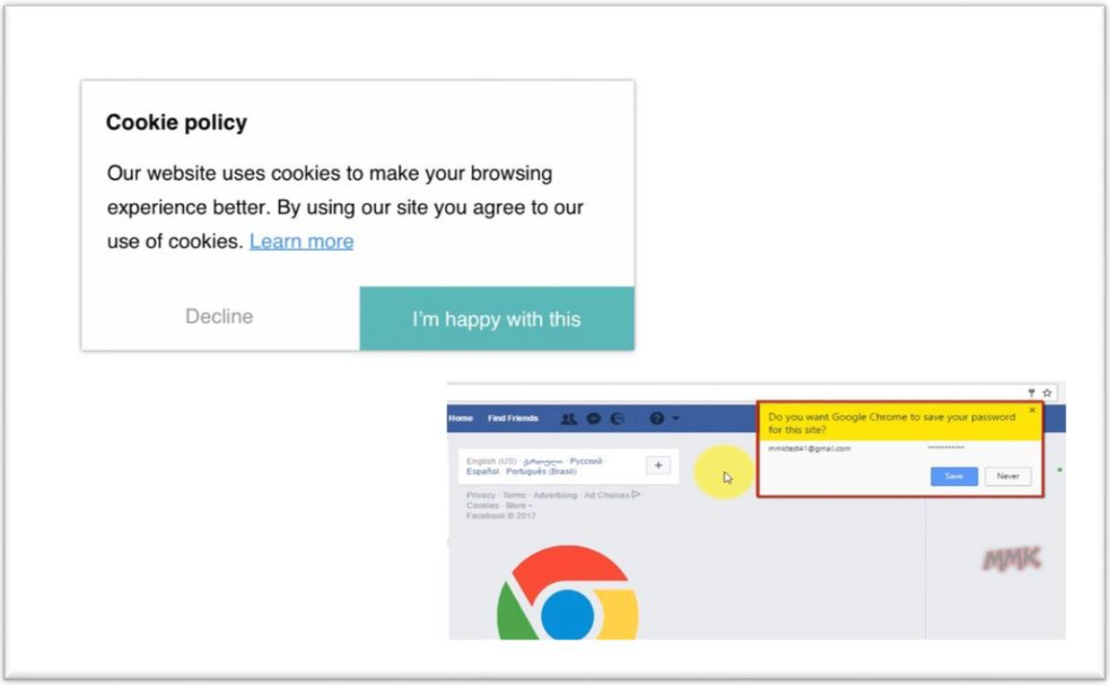
The advertisers discover consumer information by tracking their activity on the internet using monitoring technologies (cookies) for consumer profiling and presenting personalized advertising, which involves the processing of personal data of the users over time.

"Cookies" are short alphanumeric text files which are stored on the data subject's computer whenever he/she accesses certain website. They store information about the users and their preferences and this information can be re-read in future visits.

Some examples of cookies include the ones used to store login information such as username and password for the user to not have to log in every time he/she visits the website. Cookies are also used by electronic commerce websites to store items in the shopping cart during the buying process. The use of cookies to target and personalize marketing communications makes advertising more engaging for the users and brings more value to the publishers and the advertisers.

FIGURE 1

Google's privacy policy notice to its users, warning them that their website uses cookies



Purpose of Cookies. Cookies can be created by first or third parties, both used on a multitude of websites to track user behavior. They have similar purposes but are collected and used in different ways.

First party cookie: First-party cookies are directly stored by the website (or domain) you visit. These cookies allow website owners to collect analytical data, can remember language settings and perform other useful functions that provide a good user experience. For instance, if it's an online store, the website puts a cookie on your hard drive that has its own unique identification code, the site then uses this id to keep track of your session (your overall visit on the website, from start to finish) to keep track of your activities like which items you put in your shopping cart or which items you looked at or even save coupon codes for you and so on.

Third party cookie: Third party cookies are created by domains that are not the website (or domain) that you are visiting. These are usually used for online-advertising purposes and placed on a website through adding scripts or tags. A third-party cookie is accessible on any website that loads the third-party server's code. For instance, if you are browsing around a

website that has a button to like or share on Facebook embedded into it, and you clicking on it would mean that Facebook can now send their own cookies to this website in order to track your activity and most likely serve you with some targeted ads on your Facebook feed later.

Opt-out cookies. If you don't want any cookies on your hard disk, then your best option would be to delete your cookies and then block them through your browser settings. Merely deleting cookies from your hard disk is unproductive since most websites recreate deleted cookies quickly. This makes them likely to just reappear the next time you go online. On the other hand, blocking cookies inhibits websites from directly embedding cookies into your hard disk. But changing your cookie settings comes with repercussions: your online experience will change most likely in a negative way if you delete all cookies as some cookies truly enhance your online experience by saving your login details and so on. Not all cookies are privacy breaching parasites; it is mostly the third party "cookies" which are the most disturbing considering their high degree of intrusion into the privacy of users.

According to a study, by Alecia M. McDonald & Lorrie Faith Cranor from Carnegie Mellon University (2010), on the American adult internet users, it was found that users lack knowledge about what a cookie is and what are its functions and it was found that there is a gap between the knowledge users currently have and the knowledge they would need to possess in order to make effective decisions about their online privacy. This has implications for public policy, commerce and technologists. During this research, many people claimed to have never been taught about online privacy policies in their school life and it is now highly believed that there is a serious need not just for improved notice of practices, but for the education requisite to understand disclosures. After the result of in-depth interviews and an online survey focusing on participants' views of online advertising and their ability to make decisions about privacy trade-offs, this study shows that only 11% of the respondents understood the text description of the

opt-out cookies (The opt-out cookie tells the website not to install third party advertiser or other cookies on your browser) which help users make informed choices and 86% believe ads are tailored to websites they have visited in the past, but only 39% believed there are currently ads based on email content, and only 9% think it was okay to see ads based on email content as long as their email service is free. Approximately 20% of participants want the benefits of targeted advertising, but 64% find the idea invasive, with 40% willing to self-report that they would change their online behavior if advertisers were collecting data.

Targeted political advertising and Facebook

Not very long ago, advertising strategies for political campaigns primarily used approaches for getting out the votes and focusing on mass reach via shows networked at prime time at which a radio or television audience is expected to be at its highest and news programing, automated calling and direct mail. However, Political cable advertising has grown significantly year over year in both revenue and market share, even as the rest of us give up television for hours of Internet-enabled binge watching, political campaigns still cling to the allure of the 30-second TV spot. They know it's still the easiest way to reach most people at once, and especially when you are trying to persuade millions of people to vote for you.

The problem, as most other industries have figured out, is that television is kind of a risky matter, compared to all the fine-tuned ad targeting that's possible through platforms like Facebook, Google and Twitter. Social media has been well on its way to replace television as the dominant platform for campaign spending, beginning with the 2008, Obama's presidential election to 2012 Obama's presidential re-election campaign (data driven campaign) which for the first time built a vast digital operation combining a unified database on millions of Americans with the power of Facebook to target individual voters to a degree that had never been achieved before.

As stated in 'The Guardian' (2012), for every person that would log onto the Obama's re-election website on Facebook was consciously or otherwise injecting all the information that was stored publically on their Facebook page – home location, date of birth, network of friends and interests directly into the central Obama database. A digital campaign organizer who worked on behalf of Obama says. "If you log in with Facebook, now the campaign has connected you with all your relationships." The digital analysts predicted it to be the first election cycle in which Facebook could become a dominant political force with the help of a marketing strategy, 'Micro targeting' that uses people's data about what they like, who they are connected to, what their demographics are, what they've purchased and more, technique used by political parties and election campaigns now-a-days.

According to an article by Matthew Crain from Miami University & Anthony Nadler from Ursinus College (2019), digital advertising generally focuses on social media platforms because of their centrality as online spaces and their dominant position in the global advertising market. Data-driven ad technologies enhance the influence that advertisers can have on-target audiences by leveraging detailed information about individuals, often without their knowledge or consent. Data driven advertising is designed "like a one-way mirror" in which campaigns and tech platforms can see the public, but the public cannot see them. One of the most important findings of this article is that digital ad systems have been built with abilities that can easily help the political operatives to identify weak points where groups and individuals are most vulnerable, to plan and establish influence among the public. In such scenarios individual data is turned against them and is used to help the political advertisers influence their targets.

As stated in the article, in the recent times governments have begun to acknowledge and respond to an emerging set of problems associated with manipulative online political advertising. Many researchers and policy makers have used a number of terms to describe these problems. In

the wake of The BREXIT, leave EU vote and the 2016 US presidential election, the term ‘fake news’ spread around fast among the journalists and researchers to appoint the inaccurate news stories that were being widely shared on social media. These stories were mostly created by the small entrepreneurs looking for profit from click bait or partisan operatives using false news to influence the people. However, the term ‘fake news’ was confusing because it could be used to refer, quite different kinds of content, from good-faith journalistic mistakes to blatantly false news to make profit and to even news satire. Populist politicians especially seized this term quickly and started labelling any critical coverage of them as “fake news”.

The term ‘manipulation campaigns’ has been used to name a range of deceiving communication strategies that use data-driven advertising to target vulnerabilities to influence people, in attempts to shape discourse or behavior to meet strategic objectives. All the manipulation campaigns keep some aspects of their operations hidden from their targets, but they obviously do not necessarily traffic in false information. For instance, one of the most well-known controversies regarding voter manipulation was the 2016 US election, ‘The Cambridge Analytica Scandal’, a scandal which plunged Facebook into the greatest crisis in its then 14-year history involving, gathering of unauthorized data on 50 million Facebook users by a British consulting firm Cambridge Analytica that worked for Donald Trump. The Scandal played on the data-driven research tactics which helped the firm target the selected audience and bombard them with advertisements (supporting trump campaign) hence, manipulating them into voting for Trump. This manipulative campaign targeted only a particular set of people which according to them were the ‘persuadable’ (people with not so strong political opinions) and bombarded their feed with all the advertisements/messages with the hope of changing their opinions and persuading them into doing what they wanted them to do (see, by Matthew Crain from Miami University & Anthony Nadler from Ursinus College 2019).

Facebook

How Marc Zuckerberg came up with the idea of Facebook?

According to the film The Social Network 2010, on a fall night in 2003, Harvard psychology undergrad and computer programing genius Mark Zuckerberg sat down at his computer and heatedly began working on a new idea, creating an online program called 'Face mash', which allowed users to objectify fellow students by comparing photos of their faces and selecting who they deemed as 'hotter'. While Zuckerberg faced punishment from the Harvard administration and narrowly escaped expulsion from the college altogether for his actions, 'Face mash' provided the framework for what was to become the 'Facebook' we know of today.

In a rage of blogging and programming, what initially began in his dorm room soon became a global social network and revolution in communication. A mere six years and 500 million friends later, Mark Zuckerberg became the youngest billionaire in history but for this entrepreneur, success leads to both personal and legal complications.

Facebook, an American social media and technology company started in 2004 with the motive to connect people and to give them the power to build community and bring the world closer together was an instant hit especially with its continued expansion plans over the years; people were clamoring to sign up on this website and by 2007, Facebook started its own Marketplace which let users post classifieds to sell products and services. The platform soon started looking beyond personal profiles to how a business could use the site, making plans to build on ad revenues to make advertising available to even the smallest of businesses.

Facebook over the years, also started providing its advertising services to political and advocacy groups around the world with education and guidance on how to connect with their citizens and supporters on Facebook in a transparent, scalable way, regardless of their location or political affiliation by serving images, posts to a targeted audience through

the Facebook platform and ad network which eventually led to the misuse of our personal information and the infamous 2016 Cambridge Analytica Scandal.

Cambridge Analytica Scandal

Cambridge Analytica ltd. (CAL) was a British political data-analysis consulting firm that ceased to exist in 2018 over mishandling the Facebook user data, in the course of the Facebook-Cambridge Analytica data scandal. The company was partly owned by the family of Robert Mercer, An American hedge-fund manager who supports many politically conservative causes.

This political data-analysis firm worked on 2016 Republican businessman Donald Trump's campaign and claimed to have 5,000 data points on over 230 million American voters without their consent and their awareness, which it used to build extensive personality profiles for psychographic targeting i.e. targeting people according to their attitudes, aspirations and other psychological criteria, especially in the market research, which led to the great privacy breach of 2016.

CAL was a consulting firm that combined misappropriation of digital assets, data mining, and data brokerage and data analysis with strategic communication during the electoral processes. It was started in 2013 as an offshoot of a Strategic Communication Laboratories (SCL) and had later found itself in the spotlight along with the social networking corporation Facebook Inc. and a little known company called Global Science Research Ltd. (GSR) in the retrieval of personal data from up to 50 million Facebook users, amid the 2016 US presidential election and The BREXIT – leave EU vote campaign.

In May 2018, CAL and SCL (including multiple, affiliated companies, such as SCL Analytics Ltd. and SCL Commercial Ltd.) filed for bankruptcy in the United Kingdom (UK); soon afterwards, their US counterparts followed suit. They are being legally investigated in the

UK and the US (BBC 2018; Reuters 2018). Facebook CEO Mark Zuckerberg had to testify before US Congress and to justify the corporation's role in exposing users' data in a hearing at the European Parliament. Also, GSR-cofounder and University of Cambridge (UOC) researcher/lecturer Aleksandr Kogan received critical attention.

The role of academic, big data-driven research

According to a journal of Socio-political Studies by Annika Richterich from Maastricht University (2018), it was found that CAL and its parent company SCL received Facebook's data from the University of Cambridge's (UOC) lecturer and researcher, Aleksandr Kogan. In 2014, Kogan developed the Facebook personality-quiz app '*This is your digital life'* and with the help of this app he was able to retrieve data from Facebook users who installed the app and from their Facebook friends.

Kogan's work was directly inspired by a personality app previously developed and explored by some of his UOC colleagues. This quiz app originally known as 'My Personality' was developed by David Stillwell in 2007, while studying at University of Nottingham who later started working as a lecturer at UOC. In 2009, Michal Kolinsky joined the project, as a PhD student at UOC. Both the researchers were a part of the UOC's Psychometric research Centre, which is dedicated to research that focuses largely on tools and theories for psychological measurements, i.e. testing and measuring attitudes, personality traits or skills which contributed in the so called, data driven research and sparked debates about the research's effectiveness.

According to the app research by Michal Kolinsky & David Stillwell (2014), 6 million people participated in the app-based 'My Personality' questionnaires, however users were able to decide whether they would like to donate their scores and data for research purposes, indicating their consent through an opt-in statement and about 40% agreed to donate their information. 'My

Personality' project's database was partly based on the OCEAN scale for the 'big five' personality traits i.e. *openness, conscientiousness, extroversion, agreeableness, neuroticism.*

In 2014, Michal Kolinsky & David Stillwell were approached by Aleksandr Kogan, on behalf of SCL to ensure if the researchers would provide SCL with the 'My Personality project' database and model but somehow the collaboration did not emerge, with rumors from other sources stating that Michal Kolinsky and David Stillwell had ethical concerns regarding SCL's data practices and objectives and Kogan stating the otherwise, that there was a disagreement about the payment that Stillwell and Kolinsky allegedly requested from SCL.

Since Kogan couldn't get his hands on the data and the model from Stillwell and Kolinsky, he and GSR co-founder Joseph Chancellor proceeded on their own. Through their own 'This is your digital life' personality quiz app, they retrieved the data they needed and then this data was passed on to SCL through his own new founded company GSR while still working at UOC. Kogan and Kolinsky were later confronted and then accused of trying to release a "get rich quick" scheme within the department. Kogan insisted that he never received a salary from SCL, but he did concede that SLC paid GSR £230,000 at some point.

The Facebook personality-quiz app '*This is your digital life'* that were given special permission to harvest data from the Facebook users who took the quiz, helped SCL/CAL in harvesting data not from just the person who used the app or joined the app but also it would then go into their entire friend network and pull out all of the friends data as well, on an average along with the one person who took the quiz would give them access to the Facebook profiles of 300 others and if you were a friend of somebody who used the app you would have no idea that your entire data has been pulled like your status updates, likes and in some cases private messages as put by a former CAL employee and a whistle-blower, Christopher Wylie.

However these Facebook quizzes that helped CAL form personality models for all voters in the US, did not mean that all American voters were targeted equally based on their personality traits, in fact they were far from being targeted equally. The bulk of CAL's resources went into targeting those whose minds they thought they could change, called 'The Persuadables', the people with not so strong political opinions. 'The persuadable voters' were found everywhere in the country but the ones that mattered the most were the ones in the swing states such as Michigan, Wisconsin, Florida, Pennsylvania. Each of these states were broken down by precincts. There were approximately 22,000 persuadable voters in one precinct and it was all about targeting enough persuadable voters in the right precinct as stated by another CAL's former employee and a whistle-blower Brittany Kaiser.

CAL's creative team then designed personalized content to trigger those individuals and then bombard them with blogs, website, and videos, ads, every platform you can imagine until they saw the world the way CAL wanted them to see and voted for their candidate Donald Trump. The 2016 presidential election was about reaching people on an emotional level and crafting messages that appeal directly to them. Messages sent to people intended on engaging them directly by making them sad or angry at another group of people or politicians. For instance, the Trump campaign "Make America Number 1", informally termed as 'Defeat Crooked Hillary" was intended on negative campaigning to incite hatred among the people which strangely turned out to be quite successful for the Trump campaign.

Only in 2018 it was found that the CAL had been harvesting people's Facebook profile and selling the data to primarily conservative political campaigns in order to create what they were calling these psychographic targeted extremely personalized advertising often found promoting candidates like Trump and The BREXIT, leave EU vote even though CAL denies working with the BREXIT campaign.

The power of big data

In September 2016, at the Concordia Summit, a registered nonpartisan organization dedicated to actively fostering, elevating and sustaining cross sector partnerships for social impact, CAL CEO Alexander Nix talked about how "the company had harnessed the power of Big Data (the complex process of examining large and varied data sets to uncover information such as hidden patterns, unknown correlations, market trends and customer preferences that can help organizations make informed business decisions.) and psychographics in the electoral process" Alexander Nix also claimed that "by combining behavioral science, OCEAN scale for the 'big five' personality traits, big analytics and targeted political advertising messages, CAL was able to steer the 2016 election results."

The scandal around CAL, SCL, Facebook and GSR is particularly relevant, not only because of the public attention it attracted but because it speaks to the relevance of big data for politics and politics of big data. The case emphasizes the relevance of big data for contemporary politics, because of the influential narrative that data and analytics were crucial to effective political campaigning and electoral success. The case also emphasizes on the politics of big data, by once more illustrating a crucial, though still all too often downplayed and strategically neglected point, data is never neutral, no matter on what scale and how unassumingly it is retrieved i.e. it is not that data is evil or never useful, but the number should never be allowed to 'speak for themselves' because they don't tell the whole story when there are power imbalances in the collection environment. Data are normative and influential in that they are societally embedded and may be used to give credibility to claims and arguments, to advocate or undermine certain causes as stated in the journal of Socio-political Studies by Annika Richterich from Maastricht University (2018).

The scandal sparked debates on the effectiveness of the data-driven research, as according to theorists' people's desires and preferences are shaped by massive forces beyond their control and it is not merely rhetoric that individuals may fear, but already the very selection of digital content that they may or may not encounter online with respect to the recent data-driven micro-targeting strategies to address and mobilize the voters. It has also been argued that usually on-the-ground realities in comparison with the online ones are often much less precise and much less novel. The risk thus lies in transferring the credibility associated with scientific methods to ethically dubious, political data business practices.

However, 'Big data' is a broad and hyped umbrella term for digital data retrieved from various sources on a large scale. The term is commonly associated with the 'three Vs.': standing for (high) volume, variety and velocity as its main characteristics. This applies to the scientific research that may be retrieved from social net-working sites which validates the big data practices because of the public trust in science but according to some theorists, unfortunately scientists often uncritically adopt the assumptions and ideological viewpoints put forward by SNSs and data firms. This may lead to problematic entanglements between scientific and corporate practices – as also illustrated in the case of the CAL scandal.

The politics of big data is related to the predominant idea of big data's alleged superiority, notably in combination with their scientific use. Big data have been widely pitched and hyped as powerful backbone of scientific research and this image was significant for CAL's business claims as well as the uncertainty following the scandal. In addition to the significance of widespread dataism the involvement of academics and news reporting on the inspirational role of big data-driven research further fuelled the CAL controversy.

Even though CAL's dubious strategies were built upon scientific, data-driven models and methods which prove or spark discussions about its effectiveness as it proved to be successful in

manipulating the American voters at least in 2016 election and The BREXIT, leave EU campaign should not distract us from us from CAL/SCL's immoral intentions and business practices – which have been illegal. At the same time, one may hope that the controversy also functions as a reminder of the importance of vigilant, critical and media literate citizenship in the; digital age.

Rise and fall of Cambridge Analytica

In a power player's mind, to enrich yourself you need to dominate people and their thoughts and to dominate people through politics you need to modify their culture deliberately but slowly, like boiling a live lobster that becomes your dinner before he knows it. To change a culture, you need to apply a methodology that will slowly destabilize and confuse the people. In the case of CAL the goal was dominance over the individual and the mass by applying a military style methodology (i.e. to train people's brain to process information and carry out task in a certain way) to social media and big data.

To obtain the ultimate aphrodisiac of power and dominance over the masses, the book *"MindFuck" by Christopher Wylie* published in 2019 (the former director of research in SCL/CAL and a whistle-blower) is designed to show how CAL intentionally manipulated the people at critical junctures. In other words, profiled them to know their mode of behavior and play into their patterns of thought. The idea essentially is like an enhanced military strategic disinformation tactics game applied to real life.

The author, a former key component in CAL leads the reader through his journey with a firm named Strategic Communication Laboratories (SCL) founded by Nigel Oakes, which began by working to supply the U.K Ministry of Defense and NATO armies with expertise in information operations on how to tackle radicalization online by creating new tools to identify and combat internet extremism to persuade hostile audiences like 14-30 year old Muslim boys not to join Al- Qaeda with the help of essential communication warfare. SCL has worked in

Afghanistan, Iraq and various places in Eastern Europe but the real game changer, was when they started using information warfare in elections and all the campaigns that SCL/CAL did for the developing world including countries such as India (2010), Kenya (2013), Thailand (1997), Italy (2012), Colombia (2011), South Africa (1994) and many more, were about practicing some new technology on how to persuade people, how to suppress or increase the voter turnout.

For instance, CEO Nix reveals, how SCL engineered a highly successful grassroots campaign to 'increase apathy' so that young Afro-Caribbean's would not vote. In Nigeria, evidence was found that SCL used rallies by religious leaders to discourage voting in key districts. It's the kind of meddling that CAL's parent company had been doing for years in the developing world, a form of colonialism that rich countries are more accustomed to perpetrating than experiencing themselves. SCL/CAL's clients were simply treating the American population in the exact same way they would treat the Pakistani or Yemeni populations on projects for American or British clients.

In 2014, when Christopher Wylie joined the SCL it was all exciting and new for him as he thought this would break new ground for the cyber defenses for Britain, America, and their allies and confront bubbling insurgencies with data, algorithms, and targeted narratives online. Then billionaire Robert Mercer acquired the project and his investment was used to fund an offshoot of SCL, which, Steve Brannon (Chief Strategist in the administration of U.S for 7 months and former vice president of CAL) named Cambridge Analytica.

Christopher Wylie then in 2014 managed to get access to the app "This is your digital life" from Aleksandr Kogan which was technically illegal as the app was only for research purposes and especially not meant for any third party access. The app worked in concert with Amazon Mechanical Turk, or MTurk. Researchers would invite MTurk members to take a short test, in exchange for a small payment. But in order to get paid, they would have to download the

app on Facebook and input a special code. The app, which was called “This Is Your Digital Life,” would take all the responses from the survey and put those into one table. It would then pull all of the user’s Facebook data and put it into a second table. And then it would pull all the data for all the person’s Facebook friends and put that into another table. Wylie knew, it would take people sometime to see the survey on MTurk and install the app but soon enough people started downloading the app and the numbers kept increasing getting them the results they wanted to achieve. Within 2 months of the app’s launch they got access to 87 million people’s Facebook profiles because of Facebook’s loosely supervised permission procedures.

Once people’s personality profiles and other details were combined, CAL officials picked some random names and states to see what all data they had on that particular individual of that state i.e. if the name was Karen and the chosen state was Nebraska, all the people who went by the name Karen popped up with information that they had on her for instance, her photo, where she works, her kids and what school do they go to, who she voted for in 2012, and not only did they have all her Facebook data, but they were merging it with all the commercial and state bureau data they had bought as well and imputations made from the U.S. Census. They had data about her mortgage application; they knew how much money she made, whether she owned a gun. They had information from her airline mileage programs, so they also knew how often she flew and they also had a satellite photo of her house, easily obtained from Google Earth.

They had re-created her life in their computer, sitting in London while she was in another country with absolutely no clue. Alexander Nix then started randomly dialing numbers of a few people from their research to ask them questions regarding the data they had about them and it obviously turned out to be accurate.

CAL had done it. They had reconstructed tens of millions of Americans inside of a computer, with potentially hundreds of millions more. They had indeed created something so

powerful; it felt sure that it was something that people would be talking about for decades and soon enough more political parties started approaching them showing them their interest in accessing this data and they first worked on the Ted Cruz campaign and then they worked on Donald trump's 2016 Presidential election campaign on the project Alamo (associated fundraising and political advertising operation on social media platforms) spending a million dollars per day on ads.

According to Christopher Wylie, the firm became a revolving door of foreign politicians, fixers, security agencies, and businessmen with their scantily clad private secretaries in town. It was obvious that many of these men were associates of Russian oligarchs who wanted to influence a foreign government, but their interest in foreign politics was rarely ideological. Rather, they were usually either seeking help to stash money somewhere discreet, or to retrieve money that was sitting in a frozen account somewhere in the world. According to Christopher Wylie, Trump colluded with Russia during the 2016 presidential election with the goal of harming the campaign of Hillary Clinton and increasing political and social discord in the USA.

Robert Mueller (American lawyer and government official) claims in 2018, CAL was under investigation for Russian interference in 2016 presidential election – both because Nix contacted Julian Assange, founder of WikiLeaks that summer to discuss hacked Democratic (Hillary Clinton) emails to which they got access to by the Russians (as alleged by many other sources) and because of the broader questions about whether Trump‘s digital operation collaborated with the Russians in some way.

Over time, Christopher Wylie realized the "wrong doings" of the firm and confessed, "Like so many people in technology, I stupidly fell for the hubristic allure of Facebook's call to "move fast and break things. I've never regretted something so much. I moved fast, I built things of immense that I lost my moral regard towards my people and helped in hacking our

democracy." In late 2014 Christopher decided to leave the firm, however only to start his own firm which he allegedly used to compete with CAL for the 2016 Trump campaign but lost the contract and in 2018 he decided to come out as a whistle-blower and gave his testimony in the UK parliament against CAL works and exposed another former employee of the CAL named Brittany Kaiser, one of the most controversial names in the CAL scandal as she worked for CAL for more than 3 years and was also a part of the Trump campaign in 2016 but decided to quit the firm in 2018 before the scandal made the headlines for the biggest privacy breach on social media.

Brittany Kaiser**,** (A former development director of CAL.) In an explosive memoir "Targeted" published in 2019, a political consultant and technology whistle-blower, Brittany Kaiser reveals the disturbing truth about the multi-billion-dollar industry, revealing to the public how companies are getting richer using our personal information and exposing how CAL exploited weakness in privacy laws to help Donald Trump and how this could easily happen again in the 2020 presidential election.

Brittany Kaiser, a human rights activist started interning for the Obama campaign in 2007, the first time social media was used in a political campaign apart from its use to connect with friends. She created Obama's Facebook page and then along with the Obama campaign team began collecting data from people's Facebook profiles in the most rudimentarily/basic ways possible by looking at what people cared about and what were they commenting on and started categorizing the data on the basis of the information that was accessible to them and that data would end up feeding into all the emails they sent to the people making sure their conversations with them were on one on one basis so they could connect with them on a personal level.

According to Brittany, it was an extremely positive campaign; in fact they banned all hatred from their Facebook pages. However, she claimed that it was the beginning of data

collection on social media to target the users, but everything that came after the Obama election was about advanced data analytics and finding more effective ways of collecting data on citizens as, the more you know about the citizens the easier it is to engage them and persuade them.

After leaving the internship she eventually ended up meeting Alexander Nix amid her thesis during her PHD, who offered her a job in CAL in 2015 where she could really learn about data analytics which made her realize the power of big data and how they were collecting it. Kaiser claims that on the outside SCL/CAL seemed like a group of people trying to make the world a better place making the best use of technology when in real it was just an evil corporation feeding all Americans their evil works. Kaiser claimed that she always thought of Nix to be a great person and a mentor until according to her when she finally realized (which was in 2018 after working for CAL for 3 years), what a monster he was to have created what we call today "The Cambridge Analytica Scandal" and came out as a whistle blower only after being exposed by Carole Cadwalladr, a journalist and Christopher Wylie.

In the memoir "Targeted" Kaiser reveals that CAL worked for "The BREXIT" leave EU vote campaign (2015) but they quit early in the campaign as they were not paid for it which sparked concerns in the EU parliament in 2018, with EU commissioner of Justice arguing "We have to understand that these practices might have relevance for elections or referenda in Europe and if one country's elections are at risk of being manipulated, then this can also have an impact on our whole Union. And this is a big concern, in particular, ahead of the upcoming European Parliament elections."

Brittany Kaiser, in her written testimony to EU parliament in 2018 to the fake news inquiry, seems to be struck by shock by the testimony of the committee on this topic and the growing number of reports about how Facebook data was abused by Alexander Kogan, Global Science Research and CAL without users' consent, and even more shocked about Facebook's

own failures to protect their users' data, as she claims to not have been a part of the firm when the research was undertaken and to have never met Kogan, however she wrote that she could still answer questions on this topic but with no special knowledge of the datasets or their acquisition.

Kaiser also claims to have been assured by the company executives in January 2018, that they had taken appropriate action to comply with the law and contractual requirements, including deleting all Facebook data after the election. With the time she spent working for CAL and the further perspective that she had gained on the issue over the past weeks she believed she had evidence of CA obtaining, retaining and using these datasets, seemingly in contravention of legal obligations. Kaiser in her testimony also mentioned to have launched the #OwnYourData campaign at the start of April, challenging Mark Zuckerberg to alter Facebook's terms of service to give users more rights over the use and monetization of their own data.

The points mentioned below offer specific details about Facebook data issues that Brittany Kaiser wrote in her testimony to EU parliament to the fake news inquiry, 2018

a) "Access to Facebook data was a part of CAL sales and marketing "pitch" to commercial, political and defense clients throughout my time at the company – even after the request from Facebook to delete the data.

b) I never had access to the Kogan/GSR dataset on 87 million friends, or to any other sophisticated Facebook dataset; I how it had been acquired and I was told by company leadership that CAL was complying with the law and with Facebook's requirements at all times.

c) In May 2015, CAL current Chief Data Officer asked for me and two other colleagues to look through a list of Facebook groups and choose 500 of them to receive data related to the people who had liked those groups. I was told this was one of our last chances to get Facebook data. I believe now that this is later than the publicly stated date of April 2015 when the API loophole was announced to be closed.]

d) As I told The Guardian in March 2018, I was forwarded emails between CA's Chief Data Officer and Facebook in December 2015 and January 2016. Facebook asked if we still possessed the Kogan/GSR datasets; our CDO confirmed that we did; Facebook asked for them – and any models derived from these datasets – to be destroyed. The CDO then told Facebook that the data had been deleted. Following statements from former CA employees, I am now asking questions about whether this was the case.

e) I have since found another email dating from March 2016 in which another of our senior data scientists confirmed in writing that we were using some Facebook likes for modelling, two months after we confirmed that these data were deleted.

f) I should emphasize that the Kogan/GSR datasets and questionnaires were not the only Facebook-connected questionnaires and datasets which CAL used. I am aware in a general sense of a wide range of surveys which were done by CA or its partners, usually with a Facebook login – for example, the "sex compass" quiz. I do not know the specifics of these surveys or how the data was acquired or processed. But I believe it is almost certain that the number of Facebook users whose data was compromised through routes similar to that used by Kogan is much greater than 87 million; and that both CAL and other unconnected companies and campaigns were involved in these activities."

Following the 2016 data scandal, Facebook and its privacy terms and conditions have received crucial attention especially by the UK parliament and US congress for deceiving its people into believing that their data was in safe hands when in real it was being misused against them this whole time. However this leaves us bewildered with the question "was everyone so in love with the gift of free connectivity that no one bothered to read the terms and conditions?"

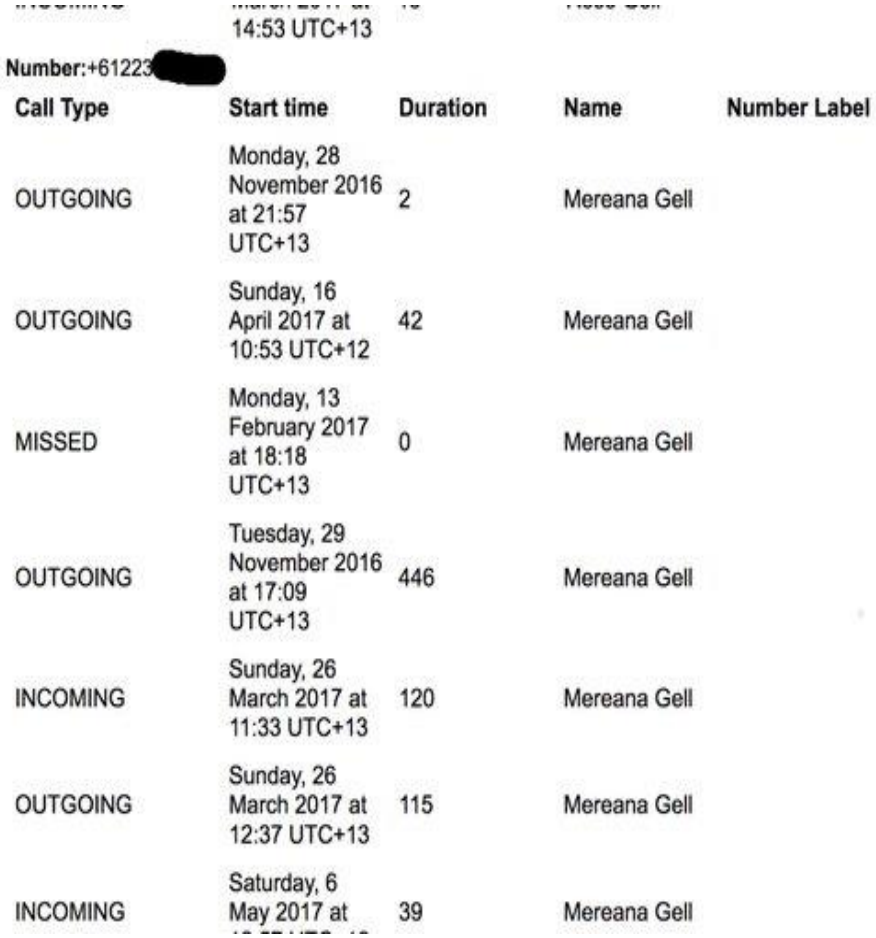
Facebook and its failure to protect user data

According to an article by Sophie Gallangher & Max Thurlow (2018) in Huffington post, it would take an average of 76 working days to read all the privacy policies you encounter on the internet in any given year, so it's no surprise that many users don't always take the time to read the fine print.

Comprising 14000 words, Facebook's terms and conditions are not briefly and clearly expressed, so if you are on a platform accessed by 1.4 billion daily active users you may want to think about whether you properly understood what you are signing up for, especially in the wake of the Cambridge Analytica Scandal.

When the scandal made headlines in 2018 one of the users named Dylan McKay, obtained his raw data when he requested the files from Facebook and posted on his twitter account which led to hundreds of people contribute in the same with their personal findings.

FIGURE 2 One Facebook user, Dylan McKay, was shocked at the information fb had on him.



	14:53 UTC+13			

Number:+61223[redacted]

Call Type	Start time	Duration	Name	Number Label
OUTGOING	Monday, 28 November 2016 at 21:57 UTC+13	2	Mereana Gell	
OUTGOING	Sunday, 16 April 2017 at 10:53 UTC+12	42	Mereana Gell	
MISSED	Monday, 13 February 2017 at 18:18 UTC+13	0	Mereana Gell	
OUTGOING	Tuesday, 29 November 2016 at 17:09 UTC+13	446	Mereana Gell	
INCOMING	Sunday, 26 March 2017 at 11:33 UTC+13	120	Mereana Gell	
OUTGOING	Sunday, 26 March 2017 at 12:37 UTC+13	115	Mereana Gell	
INCOMING	Saturday, 6 May 2017 at	39	Mereana Gell	

There was information about his calls and messages which led him to download the ZIP file of the data Facebook contained about him.

Others also found similar quantities of information when they requested the files from Facebook.

FIGURE 3

American Fiction writer and twitter user, Mat Johnson, tweeted about the data his Zip file contained.

acebook has responded in a statement, saying "the data uncovered is, and always has been, obtained through means that users themselves agreed to."

In fact, you haven't just agreed to a personal call log, but many other things the social media site has on file, including (but not limited to) your current or past addresses, your birthday, your family members birthdays, all apps you have added, places you've checked into, pending friend requests, deleted friends, your education, email address (even those you've removed), events you have been invited to, your last location, and phone numbers of people who don't necessarily have Facebook.

Facebook also records every IP address you've ever logged into Facebook from, and geographical coordinates of these logins and has facial recognition data based on photographs you are tagged in.

According to the Facebook's legal terms (Facebook, updated on 31 Jan, 2018):

Photographs - You own all of the content and information you post on Facebook, such as photos and videos (known as intellectual property or IP content), but that doesn't mean Facebook has no rights.

"You grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook," say the terms.

This license ends when you delete your account, but if your content has been shared with other people (for example, a photograph shared on multiple friend's pages) it will not be deleted. Content is only released from this once all other users that have interacted with the content have also broken their ties.

Not only that, but content persists in backup copies for a "reasonable period of time" – and funnily enough Facebook compares it to the contents of your desktop recycling bin.

Other people- It might be funny for you to tag your Facebook friends in certain posts or memes, but according to the legal terms you aren't allowed to "tag users" without their consent, or "send email invitations to non-users".

Your profile - "You have agreed not to provide any false personal information on Facebook or create an account for anyone other than yourself without permission.

You will also not create more than one personal account. And if Facebook disables your account, you will not create another one without their permission.

You have also agreed to self-police the following:

- You will not use Facebook if you are a convicted sex offender.
- You will keep your contact information accurate and up to date.
- You will not use your personal timeline primarily for your own commercial gain, and will use a Facebook Page for such purposes.

If you select a username or similar identifier for your account or page, Facebook reserves the right to remove or reclaim it if they believe it is appropriate (such as when a trademark owner complains about a username that does not closely relate to a user's actual name)."

Making money from you - Facebook's T&Cs state: "You give us permission to use your name, profile picture, content and information in connection with commercial, sponsored or related content (such as a brand you like), served or enhanced by us. This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without any compensation to you."

Deleting your Facebook "Information that others have shared about you is not part of your account and will not be deleted when you delete your account."

MARK ZUCKERBERG'S TESTIMONY TO CONGRESS FOLLOWING THE CAL SCANDAL 2018

According to 'The New York Times' 2018, Facebook's chief executive, Mark Zuckerberg, faced US Congress for the first time on 10th April 2018 over the data sharing scandal. Zuckerberg answered the questions from the Senate commerce and judiciary committees

on privacy, data mining, regulations and Cambridge Analytica during the course of the marathon five-hour hearing.

Given below are some key moments from the hearing:

Right to privacy. On being questioned upon the privacy policies by Senator Dick Durbin, Mark Zuckerberg replied stating how he believed that privacy is extremely important and understands how important it is to tell people exactly how the information that they share on Facebook is going to be used, however also agreed to the point of how long and confusing the Facebook privacy policies are.

Cambridge Analytica- Mark initially stated that Cambridge Analytica didn't use their services in 2015 and they weren't an advertiser on the platform so Facebook actually had nothing to ban. However, he later corrected his claims stating "Cambridge Analytica actually did start as an advertiser later in 2015."

"So we could have in theory banned them then. We made a mistake by not doing so. But I just wanted to make sure that I updated that because I misspoke, or got that wrong earlier."

"When we heard back from Cambridge Analytica that they had told us that they weren't using the data and deleted it, we considered it a closed case. In retrospect, that was clearly a mistake. We shouldn't have taken their word for it. We've updated our policy to make sure we don't make that mistake again."

Storing and selling personal data- Mark Zuckerberg, on storing people's personal data claimed "Yes, we store data ... some of that content with people's permission."

"There's a very common misconception that we sell data to advertisers. We do not sell data to advertisers."

"What we allow is for advertisers to tell us who they want to reach, and then we do the placement … That's a very fundamental part of how our model works and something that is often misunderstood."

On Senator Tammy Baldwin asking him whether the Cambridge University neuroscientist Aleksandr Kogan sold the Facebook data to anyone besides Cambridge Analytica. Mark Zuckerberg replied saying "Yes, he did."

However, he further commented on it saying "We're investigating every single app that had access to a large amount of information in the past. And if we find that someone improperly used data, we're going to ban them from Facebook and tell everyone affected."

Russian interference -Mark Zuckerberg claimed in the hearing that one of his greatest regrets in running the company is that Facebook has been slow in identifying the Russian information operations in 2016 stating "There are people in Russia whose job it is to try to exploit our systems and other internet systems and other systems as well."

"This is an on-going arms race. As long as there are people sitting in Russia whose job is it to try to interfere in elections around the world, this is going to be an on-going conflict."

Taking responsibility - Zuckerberg at the end takes responsibility for what happened with Facebook and confesses "It's clear now that we didn't do enough to prevent these tools from being used for harm. That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy."

New Facebook Platform Product Changes and Policy Updates- On Facebook for developers 2018, it is stated that Facebook is in continuation to build upon recent changes made, on how the platform works for developers, businesses and people by introducing the updated application program interface (API) and product changes (a set of routines, protocols, and tools for building software applications. Basically, an API specifies how software components should

interact) removing the older APIs, where if you were a developer on the platform you could get access to all the data feed in Facebook's API i.e. when you developed an app on that or when someone consented to use that app they were consenting their data to be shared with the developer and the third party developer that had paid Facebook with the opportunity to develop, but now Facebook has been winding down access to device- integrated APIs that enabled partners to provide Facebook experiences under partnership agreements. Facebook has been working closely with these partners to minimize consumer impact by providing alternative solutions where applicable or leveraging Facebook's sites and apps where relevant.

In addition, Facebook platform policies are being updated as part of these changes, including provisions addressing the transfer of data outside of your app, use of service providers, the processing of data by technology providers, and the ways Facebook monitors compliance with its terms.

However according to "The Guardian" 2020, Facebook received criticism from lawmakers and its own employees as it refuses to fact-check or remove political ads placed by politicians, as according to Facebook a politician's speech is news worthy and Facebook should not be the one to make decisions about its users speech. On the other hand, Twitter no longer allows political ads on its website as announced by the CEO Jack Dorsey in late 2019.

Along with this, Facebook also received other criticisms about its new policies which still do not satisfy and assure its users of their data safety and privacy as stated by Brittany Kaiser in her memoir "Targeted." Brittany reflects on how Facebook's privacy policies can be better and more reassuring by banning micro-targeting and political advertising from the platform but claims that Facebook would never do so because that's where it gains its revenue from, while appreciating Jack Dorsey's (CEO of Twitter) for banning political advertising until he figures out

how to moderate it. Moderating political advertising has quite a technology solution as only a tech could identify disinformation and fake news as its not within the human capacity to identify it, however Kaiser also states that it would irrational to blame Facebook and Twitter for growing a lot faster and coming across problems that were never expected. According to Brittany Kaiser the lack of internet literacy and Facebook's inability to measure hate speech will bring out the worst in the platform's misuse for the upcoming 2020 elections.

CONCLUSION

After understanding how CAL's strategic data-driven approach along with Facebook's lax polices made for the largest data violation in the history of social media one can truly understand the power of big data and social media in influencing people. Social media in today's world plays an extremely important role in people's lives. With the persuasiveness of social media across all ages, groups, more attention needs to be given to what is it doing to us as individual users. The endless stream of communication and connection provided by social media is changing the way we think and absorb information. In fact it is so easy to trigger people once you have access to their emotional pulse which has been proved to us by CAL quite well.

However, in this particular case, Facebook's lax policies and it's in ability to protect its users from external forces prove that it was not that hard to hack into people's minds as, all you need is a loophole on a social media website in order to start exploiting it. In 2016 US presidential elections people's information was stolen from them to make them elect someone as evil as Donald Trump. Does it mean that people were deceived into voting in the presidential election and UK Brexit?, does it mean that these elections were not fair to the people and Brexit vote should be taken again? As we don't even know what the people of Britain actually wanted,

it was these political data base agencies working for the Government sitting behind their computers telling people what to do.

Following the CAL scandal the question that matters the most as of now is that what about the information that CAL already has on us? Does it mean that we have lost our personal information forever to them and we are never going to get it back?

Also, not to anyone's surprise but the Facebook that stole all our data from us without any consent at some point also owns Whatsapp and Instagram with almost 1.6 billion active users enjoying the social network but little do they know what is happening with their information out on the app and we cannot even answer the question of whether social media is even a safe place anymore keeping in mind the recent data breach and the power of social media.

References

Crain, Matthew, and Anthony Nadler. “Political Manipulation and Internet Advertising Infrastructure.” *Journal of InfPolitical Manipulation and Internet Advertising Infrastructureormation Policy*, 9 (2019), 2019, p. 370., doi:10.5325/jinfopoli.9.2019.0370.

Richterich, Annika. “How Data-Driven Research Fuelled the Cambridge Analytica ...” *HOW DATA-DRIVEN RESEARCH FUELLED THE CAMBRIDGE ANALYTICA CONTROVERSY* , 15 July 2018, siba-ese.unisalento.it/index.php/paco/article/view/19554.

Beliefs and Behaviors: Internet Users’ Understanding of Behavioral Advertising

Aleecia M. McDonald Lorrie Faith Cranor

Mcdonald, A. M., & Cranor, L. F. (2010). Americans' attitudes about internet behavioral advertising practices. *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society - WPES '10*. doi:10.1145/1866919.1866929

Fincher, D. (Director), Rudin, S., Brunetti, D., Luca, M. D., & Chaffin, C. (Producers), & Sorkin, A. (Writer). (2010). *The social network* [Motion picture]. United States: Sony Pictures Entertainment.

Mark Zuckerberg Testimony: Senators Question Facebook’s ... (n.d.). Retrieved from https://www.nytimes.com/2018/04/10/us/politics/mark-zuckerberg-testimony.html

Kaiser, B. (2019). *Targeted: My inside story of Cambridge Analytica and how Trump, Brexit and Facebook broke democracy*. London: HarperCollins.

Wylie, C. (2019). *Mindf*ck: Inside Cambridge Analytica and the plot to break the world*. London: Profile Books.

Publication Manual of Fake News Enquiry,2018,p06

Nickerson, D. (2013). Political Campaigns and Big Data. *SSRN Electronic Journal*. doi:10.2139/ssrn.2354474

These Are All The Facebook Terms And Conditions You Agreed ... (n.d.). Retrieved May 20, 2020, from https://www.huffingtonpost.co.uk/entry/facebook-terms-and-conditions-you-agreed-to-when-you-opened-an-account-what-do-they-mean_uk_5ab8b719e4b054d118e47db9