People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
Amar Telidji University, Laghouat
Faculty of Letters and Languages
Department of English

Surveillance Capitalism's Influence on Personal Privacy and Intellectual Autonomy
Case Study: Cambridge Analytica and the 2016 U.S. Election

A Dissertation Submitted to the Department of English in Partial Fullfilment of the Requirements for Master Degree in Civilization and Literature

By:

Zakaria Chellali

Board of Examiners:

- Dr. Khalfa Sayeh, University of Laghouat, Chairman
- Dr. Mihoubi Ahmed, University of Laghouat, Supervisor
- Dr. Seddiki Mohamed, University of Laghouat, Examiner

2023 - 2024

Declaration

I hereby declare that the substance of this dissertation is entirely the result of my investigation and that due reference or acknowledgement is made, whenever necessary, to the work of other researchers.

Date: September 25, 2024

Signed: ……..

Dedication

This work is dedicated to my mother and father.

Acknowledgements

My deepest gratitude goes, first and foremost, to Allah Almighty.

I would like to thank my teacher and supervisor, Dr. Mihoubi, for his invaluable guidance.

My warmest gratitude and regards go to all my teachers.

Kind regards to the members of the jury.

Abstract

The dawn of the 21st century witnessed two developments that shaped the world we live in today. The first was the September 11 attacks, and the second was the emergence of a new market called surveillance capitalism. However, people around the globe do not seem to be as sentient to the latter's reverberations as they are to the former's. This study aims to introduce surveillance capitalism to the public by uncovering the mechanism through which this market functions, its effects on personal privacy and intellectual autonomy, and its repercussions on the collective mind in general by tracing back and analyzing the involvement of Cambridge Analytica in the United States' 2016 presidential election when the consulting firm conducted what would be seen later as one of the instances in which surveillance capitalism blatantly manifested itself. This study will take a mixed methods form in which qualitative and quantitative data will be collected, discussed, and analyzed. This study found that surveillance capitalism is a detrimental menace to anything related to liberty, ranging from the right to privacy to the right to vote. The study also found that corporations that constitute the market of surveillance of capitalism have a great influence within the decision-making rooms in the United States. This influence sabotages any attempt to pass regulations that would limit, if not curb, the unethical misconducts of surveillance capitalism.

Keywords: Surveillance Capitalism, Cambridge Analytica, personal privacy, intellectual autonomy, United States' presidential election

الملخص:

لقد شهد مطلع القرن الحادي والعشرون إثنان من التطورات التي كان لها دور في تشكيل العالم الذي نعيش فيه اليوم. التطور الأول كان هجمات الحادي عشر من سبتمبر، أما الثاني فكان ظهور سوق جديدة تعرف برأسمالية المراقبة. غير أنه لا يبدو أن للناس حول العالم وعي كاف يمكنهم من إدراك تداعيات الثاني بقد إدراكهم لتداعيات الأول. تهدف هذه الدراسة لتقديم رأسمالية المراقبة لعامة الجمهور عبر إماطة اللثام عن الظاهرة لمعرفة آلية عملها وأثرها على خصوصية الفرد وإستقلاله الفكري وتداعياتها على العقل الجمعي بصورة عامة عن طريق إقتفاء أثر كامبريدج أناليتيكا أثناء تورطهم في الحملة الإنتخابية للرئاسة الأمريكية سنة 2016 أين قامت الشركة الإستشارية بما أصبح يشار له على أنه أحد الحالات التي تجلت فيها رأسمالية المراقبة للعلن بشكل صارخ. هذه الدراسة مندمجة، حيث سيتم من خلالها جمع بيانات نوعية وبيانات كمية في الآن ذاته ومن ثم مناقشتها وتحليلها. لقد توصلت هذه الدراسة أن رأسمالية المراقبة تعتبر تهديدا خطيرا على كل ما يمت بصلة للحرية بمفهومها الواسع، إبتداءً بالحق في الخصوصية وإنتهاءً بالحق في التصويت. لقد وجدت هذه الدراسة أن للمؤسسات التي تشكل نواة لرأسمالية المراقبة نفوذا هائلا داخل غرف صناعة القرار في الولايات المتحدة. هذا التأثير يقوم بإفشال أية محاولة لتمرير قوانين تكبح جماح الممارسات الغير أخلاقية لرأسمالية المراقبة أو تحد منها على الأقل.

Résumé:

L’aube du 21e siècle a été marquée par deux évolutions qui ont façonné le monde dans lequel nous vivons aujourd’hui. Le premier était les attentats du 11 septembre, et le second était l’émergence d’un nouveau marché appelé le capitalisme de surveillance. Cependant, les gens à travers le monde ne semblent pas être aussi sensibles aux répercussions de ce dernier qu’à celles du premier. Cette étude vise à introduire le capitalisme de surveillance au public en dévoilant le mécanisme par lequel ce marché fonctionne, ses effets sur la vie privée personnelle et l’autonomie intellectuelle, ainsi que ses répercussions sur l’esprit collectif en général, en retraçant et en analysant l’implication de Cambridge Analytica dans l’élection présidentielle américaine de 2016, lorsque la société de conseil a mené ce qui serait par la suite considéré comme l’une des manifestations les plus flagrantes du capitalisme de surveillance. Cette étude adoptera une approche mixte dans laquelle des données qualitatives et quantitatives seront collectées, discutées et analysées. Cette étude a révélé que le capitalisme de surveillance est une menace néfaste pour tout ce qui touche à la liberté, allant du droit à la vie privée au droit de vote. L’étude a également révélé que les entreprises qui composent le marché de la surveillance du capitalisme exercent une grande influence au sein des salles de décision aux États-Unis. Cette influence sabote toute tentative de passer des réglementations qui limiteraient, sinon freinerait, les comportements contraires à l’éthique du capitalisme de surveillance.

List of Tables

List of Figures

Table of Contents

General Introduction

Of all the fundamental rights humans can possess, the right to personal privacy is the foremost essential, as individuals from an early age cannot grow to build a solid personality without a haven of solitude that is relatively distant from others' observation and intervention. Such space of privacy is the very bedrock upon which an individual's intellectual autonomy (individuals' sovereignty over their mind and their ability to think independently) is built. This means that one is only as intellectually autonomous as how secluded his or her personal private space is. However, modern states and sub-state actors, driven by their impulse for totalitarianism and large-scale profit, have developed, thanks to new technological breakthroughs, different modus operandi within recent decades to deprive citizens of their right to privacy.

Neil M. Richards, law professor at Washington University School of Law, explains that states tend to have an obsession of knowing what their citizens are up to in their private realms, and, as a result, each state establishes a surveillance program that matches its degree of obsession. Richards explains that surveillance, in general, comes chiefly in three manifestations; it can either be a totalitarian Orwellian surveillance; or, at a lesser degree, a surveillance established with objective to react to people's behaviors; or one established to modify people's behavior. This, Richards argues, can be excessively harmful on individuals as it jeopardizes their ability for intellectual development and can have a dangerous outcome on the foundation of civil liberties.

On the other hand, sub-state actors, particularly giant technology companies, have been developing tremendous beyond-state capabilities to conduct wide-scale surveillance on citizens for main purpose of revenue. It wasn't until the recent few years that scholars

could finally point their fingers to this silently-growing dystopian phenomenon which they refer to as *surveillance capitalism*.

The Term Surveillance Capitalism was introduced for the first time in 2014 by John Bellamy Foster, a sociology professor at the University of Oregon, and Robert W. McChesney, a communication professor at the University of Illinois, in an article in the *Monthly Review* Magazine. Foster and McChesney argue that the United States of America has merged into a warfare state within the first quarter-century after World War II. This has not only made the military-industrial complex an essential constituent in the country's economy but also a rogue force that reshaped the United States' model of capitalism with the aim to parallel arms production and demand. In order to achieve this objective, Foster and McChesney elaborate, the United States created three surplus-absorption mechanisms: overconsumption, investment, and financialization. Coinciding with technological evolution, computers and the internet specifically, this granted the government access to new far-reaching implementations of surveillance that covered three corresponding domains: militarism, the media system and corporate-based marketing, and finance. This makes a warfare state, as Foster and McChesney claim, both an imperial state by constantly waging wars on external enemies to keep the cogs of its military-industrial complex turning, and a totalitarian state by constantly surveilling its own discontent population in order to keep a tight grip over their lives. This, according to Foster and McChesney, is what makes a warfare state to always morph into a surveillance state.

Shoshana Zuboff, professor emeritus at Harvard Business School, defines surveillance capitalism as a digital mutation of classical capitalism that relies on a new logic of accumulation: a human-behavior-based data — data predicated on the everyday human

interaction with internet-connected digital devices — harvested and amassed to be used as a source of raw material to produce financial profit and alter human behavior. Zuboff argues that the vast majority of online-based companies and start-ups constitute the market of surveillance capitalism. Furthermore, the professor continues to construe the essence of surveillance capitalism by juxtaposing it as a structure with George Orwell's Oceania where rigorous surveillance is conducted by the state leader referred to as *Big Brother*. On the other hand, in the case of surveillance capitalism where there is no deterring authority, Zuboff refers to private companies that constitute the new market as *Big Other*; an organism that reduces the human experience, which is data based on personal information and behavior, into a commodity.

To a greater extent, personal privacy and intellectual autonomy are interconnected as the erosion of the first can be detrimental to the second, Carissa Véliz, an associate professor of philosophy and ethics at the University of Oxford, indicates. To elucidate this notion, Véliz sets the example of voting booths where a voter enters a tiny space made up of three walls and a curtain in order to have their privacy; such privacy eliminates any form of external pressure which makes the voter independently make up his or her mind. Furthermore, Véliz stresses that privacy is as collective as it is individual. This means that an individual is part of a society, and when an individual's personal privacy is exposed by a government or a technology company, such institutions can have an approximate idea of the surrounding people.

Definitions and points of view mentioned thus far were initial attempts to come as close to materializing the new and vague concept of surveillance capitalism. However, these studies mainly focused on surveillance capitalism from the angle of its functionality and

unethicality. This study will try to make sense of surveillance capitalism's nature and gauge the extent of its detrimental effect on the individual and the collective mind. In order to achieve that, this study will first examine the layers of soil overlapped through the decades upon which surveillance capitalism thrived; that is to say, the sequential historical periods and events in the United States that paved the way for the emergence of surveillance capitalism starting from the pre-World War I period.

This study aims to illustrate how the market of surveillance capitalism functions and identify the main players that constitute this market. Furthermore, this study intends to expose the illegal practices carried out by the United States Government agencies and large technology companies that violate the very essence on which the country was established: the United States Constitution, and, most specifically its Fourth Amendment. Moreover, this research aims to gauge the detrimental effect of surveillance capitalism on personal privacy and intellectual autonomy of individuals and societies by shedding the light on the misconducts carried out by the disreputable consulting firm known as Cambridge Analytica during the United States 2016 presidential elections. Additionally, this study will probe the relationship between the modern individual's insatiable need for convenience and how technology companies heavily feed on that urge.

This Study orbits around a central question: To what extent can surveillance capitalism threatens personal privacy, intellectual autonomy, and civil liberties in general? The study's sub-questions are as follows:

1 – Where did surveillance capitalism come from?

2 – How does Surveillance Capitalism function?

3 – Why does surveillance capitalism seem to be immune from government's regulations?

4 – How did Cambridge Analytica operate during Donald Trump's presidential campaign in 2016? And how effective it was?

5 – Can surveillance capitalism and healthy democracy coexist?

The study hypothesizes that:

1 – Surveillance capitalism is an outcome of decades of privacy violations by the successive United States' cabinets.

2 – The market of surveillance capitalism functions through secretive and devious methods that allows technology giants to extract immense amount of data from individuals without their rational and direct consent.

3 – Surveillance capitalism's immunity from restrictive regulations comes from its lobbying coalition operating within the United States' government.

4 – Cambridge Analytica, the infamous consulting firm, carried out its job for Donald Trump's 2016 presidential campaign in methods that do not conform to decent moral standards; thus, representing the perfect microcosm of surveillance capitalism. Furthermore, this study hypothesis that Cambridge Analytica had a key role, one way or another, in the outcome of the United States' 2016 presidential election.

5 – Democracy and surveillance capitalism cannot be practiced together.

This study will be both exploratory and descriptive which takes an analytical approach to discover and understand the newly rising market of surveillance capitalism. Correspondingly, this study will be both qualitative and quantitative in which historical and statistical data will be collected, discussed, and examined based on prior hypotheses. Also, an extensive number of figures in images of graphs, illustrations, advertisements and maps

will be displayed and discussed in order to have a deeper understanding of the issue and its repercussions.

This study will be composed of three chapters. The first chapter will showcase the historical background of surveillance programs leading to privacy violations in the United States and, eventually, resulting in the rise of surveillance capitalism. The second chapter will dive deep into explaining the mechanism by which surveillance capitalism functions and the unethical means by which players of the market treat personal data. Finally, the third chapter will investigate Cambridge Analytica's expedition within Donald Trump's 2016 presidential campaign, their misconduct, and their role in swaying the presidential election.

Chapter One:
A Historical Background
of
Surveillance Capitalism

But nothing is so permanent as a temporary government program.

— Milton Friedman, *Tyranny of the Status Quo*, 1984.

Introduction

Inarguably, the United States of America is not only the birthplace of surveillance capitalism but also the country where the first large-scale surveillance programs took place. This can be a solid indicator to link the newly formed manifestation of capitalism led by big giant technology corporations to the misconducts practiced by the United States government at the beginning of the twentieth century. Such practices blatantly contradicted the Third and Fourth which protect the properties of citizens and their right to privacy respectfully. So, from what point did surveillance programs start taking place in the United States? In other words, who pushed the first piece of domino?

1.1. The First Implementations of Large-Scale Surveillance in the U.S. (1900s-1910s)

1.1.1. The Bureau of Investigation and the Post Office

Peter Conolly-Smith, professor at Queens College in New York City notes that the alliance between the newly-born Bureau of Investigation (the germ of the Federal Bureau of Investigation) and the Post Office Department before and during the United States' involvement in World War I birthed the first domestic surveillance program in the country. (Conolly-Smith 7) The Bureau of Investigation was created on July 26, six years before World War I, when the Department of Justice permanently hired ten former Secret Service employees to join the Office of Chief Examiner Stanley W. Finch, which had been newly provided with a small group of federal investigators under the command of U.S. Attorney General Charles J. Bonaparte.

With a manpower of no more than 34, the Bureau did not seem to have much to offer and it mainly focused on investigating criminals who moved through the state borders in order to dodge prosecution. ("FBI Founded") This was true until Congress passed the Mann Act, also known as

the White-Slave Traffic Act on June 25, 1910, which prohibited interstate and foreign transportation of women for the purpose of "prostitution and debauchery, or for any other immoral purpose," and set a violation fine up to $5,000 (the equivalent of $165,000 in 2023) and imprisonment for up to five years. This legislation expanded the Bureau's authority, which led to a wide campaign of arrestments and gradually raised the apparatus to prominence, especially after the arrest of African-American boxing heavyweight champion Jack Johnson. (PBS, 2022)

On June 30, 1916, an enormous explosion wiped the Black Tom Island, the largest munition depot in the country at that time, off the map, and the Statue of Liberty, about one kilometer away, was severely damaged by the explosion's shrapnel. The explosion had a massive impact it was felt as far away as Maryland (288 km), and the destruction resulted in an approximate damage of $20 million (the equivalent of $560 million in 2023). It was found after investigation that the incident had been carried out by German agents as the location was a supply point for large shipments of munitions, explosives, and gunpowder needed by the European Allies on the other side of the Atlantic. (Tagg; "Black Tom Island Explodes") This act of sabotage led to the expansion of the Bureau's authority to cover the investigation of acts of sabotage committed by foreign agents. (Capello 77-78)

1.1.2. The Espionage Act (1917)

Eight months later in April 1917, the United States declared war on Germany and with that President Wilson's inclination to subdue the nation under suppression and censorship was demonstrated in his war declaration when he stated, "If there should be disloyalty, it will be dealt with a firm hand of repression." This resulted in the passage of the sweeping Espionage Act on June 15, 1917. The third section of the new legislation aimed to single out any voices of dissent within the American public and silence them called for a fine of up to $10.000 (the equivalent of

$240.000 in 2023), or/and twenty years of imprisonment for acts that might get on the way of the war efforts ranging from "wilfully make or convey false reports or false statements [*sic*]" that can hold back the military's success to "wilfully make or convey false reports or false statements [*sic*]" that may obstruct the conscription process for the army. ("The Espionage Act of 1917")

Consequently, this gave the Post Office the right to violate citizens' privacy by peeking through the mail to search for prints suspected of violating the new law by holding anti-American sentiments in its folds and rendering any print that does not match the government's narrative unmailable, which was true for fifteen socialist publications that were banned merely within the first month. The Espionage Act proved to be effective for the government to imprison vocal dissidents who violated the law and proactively curb any further dissent by discouraging the silent majority from speaking up as the conviction rate[1] of violation reached 50% throughout the war. (Conolly-Smith, 9,12)

1.1.3. Trading with the Enemy Act (1917)

Shortly after, Congress passed the Trading with the Enemy Act on October 6, 1917, with section 19 declaring that individuals and entities who "print, publish, or circulate" any "news item, editorial or other printed matter" written in foreign languages regarding the policies of the United States government in particular and governments of countries involved in the war, in general, are compelled to file a complete genuine translation with the local postmaster, otherwise the written material would be considered nonmailable and shall be banned from being published in the future. ("Trading with the Enemy Act of 1917" n.d.)

[1] **Conviction rate:** A number, usually presented as a percentage, that indicates how frequently arrests in a given community lead to actual criminal charges

However, news regarding the war printed in English were susceptible to the procedures as well, and their publishers had to keep submitting daily copies until they deemed loyal, thus, privileged with exemption from undergoing the laborious daily process. And because the hands of censorship tend to ceaselessly reach over and cover as much area as possible, the law, as admitted by the Post Office Department's Solicitor General, Judge William H. Lamar, was made quite loose and open for interpretation; this made religious, ethnic, cultural, and feminine journals, print their way to the ban-list. When questioned by Congress concerning the criteria in which they follow in order to detect when a printed work is violating the law, Postmaster General, Albert S. Burleson answered, "to say that this Government got in the war wrong, that it is in it for the wrong purposes, or…[that it] the tool of Wall Street or the munitions-makers." He added, "there can be no campaign against conscription or the Draft Law, nothing that will interfere with the enlistments or the raising of an army." Because censorship naturally calls for surveillance and vice versa, those who had been banned from publication by local postmasters, as well as their recipients, were put under the watch by the Bureau of Investigation. (Conolly-Smith 9-10, 14)

1.1.4. American Protective League (1917)

The Bureau, having a limited number of agents and avoiding any legal troubles, relied on an organization called the American Protective League, which had massive personnel of 250.000 ultra-patriotic volunteering citizens operating as informants, to conduct large-scale surveillance on citizens. The APL's vigilantes were deeply permeated within American society and existed in almost every corner of the country; they led ordinary citizens to imprisonment for up to five years merely for uttering words of slight resentment towards the government's policies concerning the war. Furthermore, members of the APL conducted many illegal actions on behalf of the Bureau's agents, such as searching trash cans in private properties, broking into houses, as well as

wiretapping telephone lines, and embedding Dictaphones[2] inside work offices with the aim of finding incriminating evidence that would later be used in court. Citizens who fell victim to such acts were legally crippled as they could not sue the Bureau's agents, for they had not conducted the transgressions themselves; they only received the evidence from some unknown APL members. (12-14) This Orwellian atmosphere, where ordinary citizens, journalists, activists, union members, and scholars felt monitored by the APL's vigilantes, but no one knew who they were, created a sense of paranoia within the society, and even compelled many prominent authors from wide spectrum of ideologies, such as African-American sociologist, socialist, and civil rights activist W.E.B Du Bois, the Jewish Daily Forward newspaper editor and novelist, Abraham Cahan, and settlement activist and founding member of the Women's Peace Party, Jane Addams to practice self-censorship to avoid the risk of being stigmatized as anti-American. (12-13)

1.1.5. Sedition Act (1918)

On May 16, 1918, six months ahead of the Great War's end, Congress passed the Sedition Act as an extension to the Espionage Act to further tighten the state's iron grip on liberties by targeting the freedom of speech and freedom of the press. The law set a fine of up to $10,000 or/and imprisonment for up to twenty years for anyone who disseminates fake news along with anyone who "shall willfully utter, print, write, or publish any disloyal, profane, scurrilous, or abusive language" towards the government, its policies, or the military. ("Sedition Act of 1918") The penalties introduced in the Sedition Act were already being practiced off the books through the few preceding years, and the law retroactively legalized them. Not long thereafter, World War I officially ended on November 11, 1918. Nevertheless, wartime

[2] **Dictaphone:** An archaic tape device that was used to record verbal dictations and then reproduce it for retyping.

surveillance continued to slither by through the following years as Bolsheviks became the new boogeyman in what was called the first Red Scare; a period of subversions and bombings carried by far-left movements that rose to the scene creating political and social turbulence. As a consequence, the Bureau of Investigation further expanded its authority by creating and indexing catalogs and files of subversives as well as carrying out large-scale raids and interrogations that did not align with the Fourth Amendment. (Capello 73)

As it marked the end of the first Red Scare, the year 1920 witnessed the start of the Prohibition Era, during which the Bureau of Investigation along with local police departments extensively wiretapped calls of bootleggers, who used telephones to communicate with producers, distributors, and consumers. This abuse of power resulted in public resentment that pushed U.S. Attorney General Harlan Friske Stone in 1924 to prohibit the Department of Justice from wiretapping, and by 1928, over half of the U.S. states criminalized wiretapping. (Price 34; Morgan 4)

1.2. From the Roaring Twenties to the Cold War (1920s-1970s)

1.2.1. Olmstead v. United States (1928)

In the same year, the debate over privacy reached the Supreme Court with a case known as Olmstead v. United States when federal agents conducted warrantless wiretapping on Roy Olmstead's house and work office telephones to find proof of his involvement in the illegal liquor business. After collecting enough convicting evidence through Olmstead's conversations, federal agents arrested him. This led the Supreme Court to hold a discussion in aim to decide whether the government violated the Fourth Amendment. Eventually, the Supreme Court ruled that there had been no violation of the Fourth Amendment, for there was no actual physical trespassing to private

properties as the telephone lines wiretapped by the federal agents were outside Olmstead's house and office. ("Olmstead V. United States")

1.2.2. The Federal Communication Act (1934)

The Supreme Court's decision was deemed controversial by the general public, which prompted Congress in 1934 to enact the Federal Communications Act with the ineffective Section 605 prohibiting government officials only from revealing intercepted communication in court and not from the act of interception itself. This, alongside Olmstead v. United States, gave the Bureau of Investigation, which would be renamed "the Federal Bureau of Investigation" a year later, a solid legislative ground to expand wiretapping. (Morgan 6-7)

Before the United States' entrance to World War II, the FBI's main focus was eradicating individuals and organizations leaning towards both the Axis powers and the Soviet Union, ideologically or even sympathetically. The Bureau was granted an under-the-table authority by President Franklin D. Roosevelt to peek through the mail and conduct wiretapping. Furthermore, in May 1940, President Roosevelt gave the FBI the green light to carry out warrantless electronic surveillance to cover anyone suspected of holding radical anti-American sentiments. (Morgan 2)

1.2.3. The National Security Act (1947)

After the end of the Second World War, a cold war, heavily based on espionage, between the United States and the Soviet Union was looming on the horizon. As an early reaction, President Harry S. Truman signed the National Security Act in July 1947, which gave birth to the Central Intelligence Agency. The act underlined the framework of the CIA as an institution responsible for gathering intelligence concerning foreign threats as well as conducting secret operations abroad. ("Establishment of the CIA;" "Britannica")

1.2.4. Operation CHAOS (1967-1974)

However, the newly born apparatus did not seem to abide accordingly, as it went far beyond the line. Starting from the late 1960s to the early 1970s, the CIA, by the orders of President Lyndon B. Johnson and President Richard M. Nixon, covertly conducted what was known as *Operation CHAOS*. Aiming to single out movements with the slightest foreign connections, CIA agents penetrated the so-called "New Left" with great emphasis on African American movements that stood at the epicenter of the civil unrest, such as the Black Panther Party and the Southern Christian Leadership Conference. Through surveillance, the CIA indexed over 300,000 names with fragile proofs of foreign connection, from which 7,200 citizens had more detailed files. The White House pushed the CIA to further deepen their operation regardless of the latter's reports that concluded that there were no foreign connections found whatsoever, as former CIA agent, Frank Rafalko, writes:

> Each time we reported that there was no evidence of foreign control within the domestic student and black militant groups, the White House reaction was one of skepticism… It was back to the drawing board each time. And each time, we had to expand our horizons, to reach further and look at every dissident to try to detect any foreign contact and what that contact meant. In the end, we were trying to defend our conclusion—we were trying to prove a negative.

In 1974, Operation CHAOS was officially aborted with no outcome other than more violations against the constitution. (Janos)

In an attempt to increase transparency within the federal domain, and to control the surge of indexing caused by the flow of records obtained by federal agencies, Congress passed the Privacy

Act in 1974, which gave citizens the right to acquire data collected about them. The Privacy Act, however, did not cover state or local agencies nor the whole private sector. Moreover, according to the act, the request of data revelation would only be accepted if it did not counterpose the basis in which the data had been collected in the first place. Another concerning outcome of the act was the ability in which a third party could legally obtain data about citizens on request. By and large, the Privacy Act was another major step in the U.S. government's journey to institutionalize surveillance (Morgan 10-11)

1.3. The Patriot Act (2001)

It wasn't more than six weeks after the attacks that led to the collapse of the World Trade Center on September 11, 2001, that the United States' Congress passed the controversial *Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, also known as the Patriot Act; the straw that broke the foundations of personal privacy in the country. (Lind) The new law gave federal agencies like the FBI unlimited access to people's electronic devices. Thanks to the new law, the Bureau of Investigation was able to issue NSLs (a national security letter) to force companies to give in telephone, internet, and banking data about their customers under the pretext of countering terrorism. Interestingly, more than 143.000 NSLs had been issued between 2003 and 2005. Some of which concerned immigration, others concerned fraud and money laundering, but none of which was issued for terrorism. And it is noted that since its creation 23 years ago, less than 1% of the Patriot Act implementations tackled terrorism. ("Surveillance Under the Patriot Act;" "National Security Letters")

1.4. The Rise of Surveillance Capitalism (2000s)

Surveillance took a drastic turn when Google, the newly rising tech company, realized that data generated by users could be highly profitable. Google, which was founded on September 4, 1998, by Ph.D. students at Stanford University, Larry Page and Sergey Brin, introduced a breakthrough innovation called PageRank; an algorithm that, according to the corporation, "works by counting the number and quality of links to a page to determine a rough estimate of how important the website is." This feature quickly elevated Google to the highest rank of reliability in the world of search engines, especially among academics, for its ability to organize results based on the significance of websites. However, this was a free service, and Google, unable to charge money for it in order not to lose competition with its counterparts, needed to find a business model[3] as the start-up company was in desperate need of a source of income, especially with investors pressurizing with threats to withdraw their funds. (Véliz 17-18; "Page Rank Algorithm and Implementation")

Other search engines profited from advertisement instead of charging for fees, but Page and Brin, in a paper written in 1998, demonstrated their unenthusiasm towards introducing ads to their platform, "… we expect that advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers." Page and Brin continued to elaborate on their standpoint, "… we believe the issue of advertising causes enough mixed incentives that it is crucial to have a competitive search engine that is transparent and in the academic realm." (Storelli)

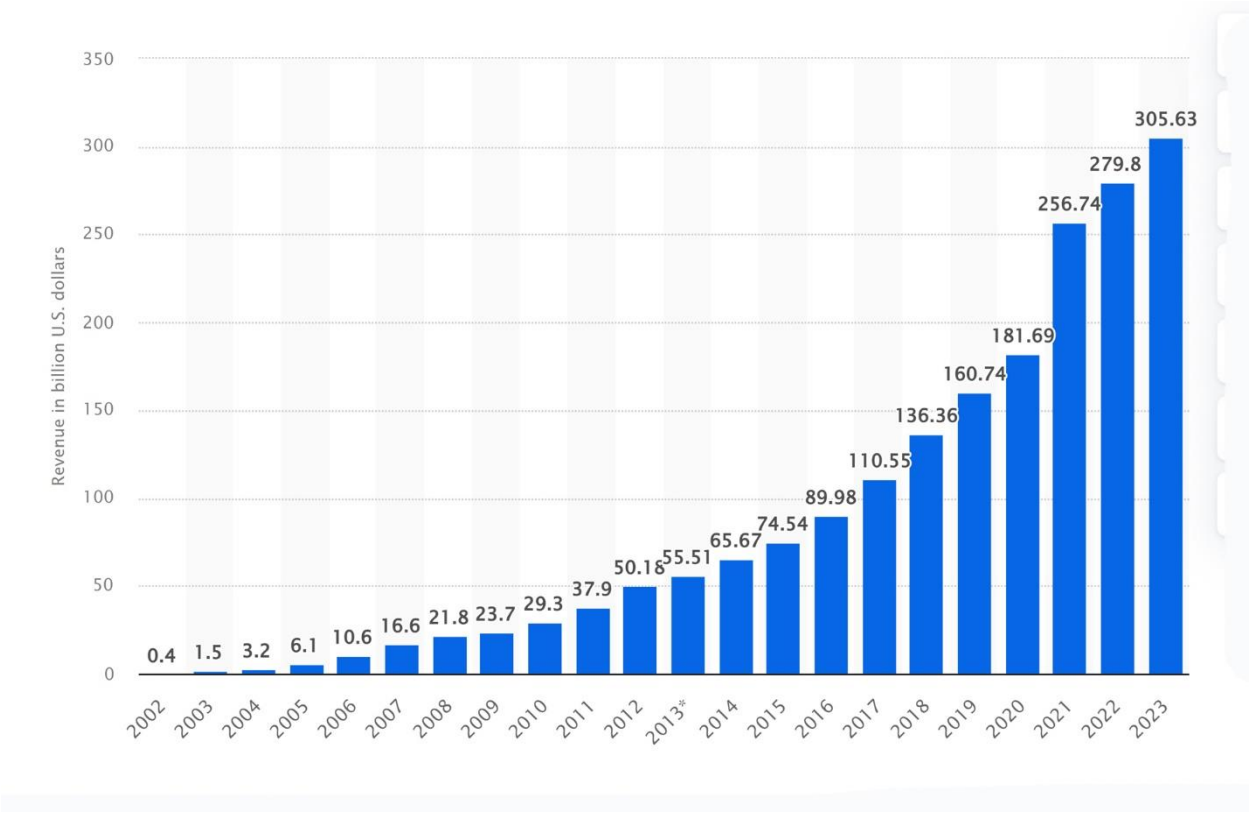
Google had to choose between providing adless quality services or making a profit. Eventually, they chose both options by creating a unique advertising system: AdWords (known

[3] **Business Model:** A business model is a strategic plan of how a company will make money. The model describes the way a business will take its product, offer it to the market, and drive sales.

today as Google Ads). Unlike the costumery advertising system used online back then, which gave advertisers the privilege to choose the best positions to place their ads, AdWords functions by prioritizing ads that receive the highest number of clicks. Google, realizing that advertisers were clicking their ads to get more views, turned AdWords into a bidding system; advertisers had to provide a bid for the sum of money they were to pay for a single click on their ads. At that point, AdWords seemed to generate a business relationship based on trilateral satisfaction between Google, advertisers, and users, but the latter had to give up one of the most important aspects that shape the human essence: privacy. Google's annual revenues surged as the company started utilizing users' personal data, which was once used in a limited scope as feedback to help companies improve their service, to create personalized advertisements, and with that, the company began to know more than it should about its users as they interacted with the search engine. On March 4, 2003, Google announced a new advertising system called AdSense to complement AdWords; the latter would only display advertisements on Google's website, and the first started putting them on other web pages. Thanks to this, Google's annual revenue tripled during AdSense's first year (Véliz 18-19; Bales; "Annual Revenue of Google from 2002 to 2023;" Wood). (See Figure 1).

Figure 1

Annual Revenue of Google from 2002 to 2023 (In billion U.S. dollars)



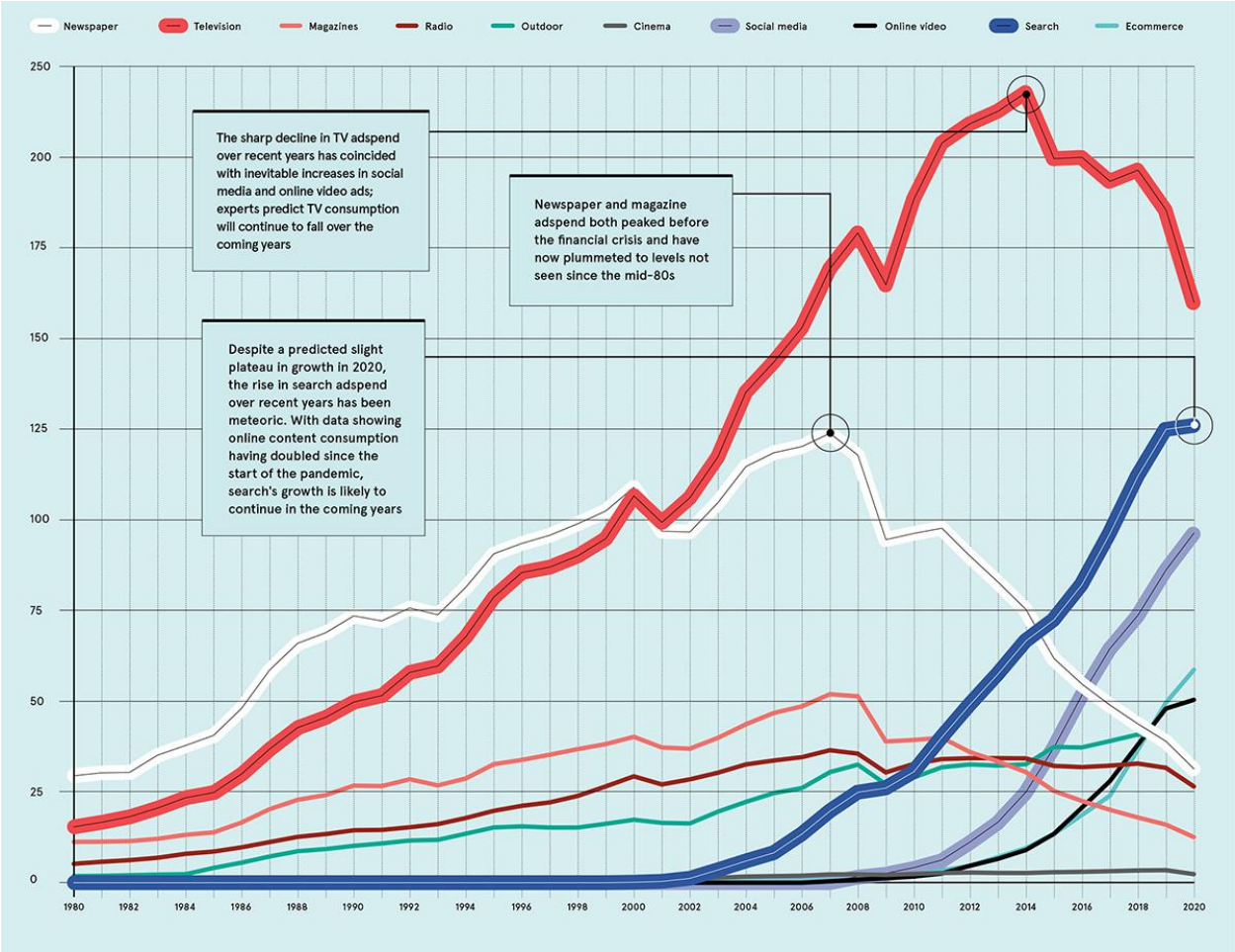
Source: Statista

https://www.statista.com/statistics/266206/googles-annual-global-revenue/

Incentivized by Google's profits, other technology companies soon began to migrate towards the new prosperous surveillance economy by adopting the rising giant's business model. This resulted in the growth of online advertisement at the expanse of deep-rooted advertising outlets, such as newspapers (Véliz 18-19; Bales; "Annual Revenue of Google from 2002 to 2023;" Wood). (See Figure 2).

Figure 2

Evolution of Global Spending on Advertisement From 1980 to 2020



Source: Visualcapitalist

https://www.visualcapitalist.com/evolution-global-advertising-spend-1980-2020/

In 2007, Google continued advancing in its quest towards the surveillance economy by buying DoubleClick, an advertising company that used “cookies” (a small piece of data used by websites to track users’ personal activities as they surf the internet) for more efficient targeted advertisement. As a result, Google has become able to collect data about users and monitor their online activities even if they do not click on advertisements. On the other hand, users were satisfied

with the new state of convenience online and did not seem to consider the magnitude of the exchange they signed up for, nor what they were giving up in order to receive such adequate services. Google, as the rest of other technology companies, made sure to maintain the new business model as clandestine as possible. (Véliz 19-20)

1.4.1. Setting the Psychological Ground for Surveillance Capitalism

However, this secrecy slowly started to unveil, which led technology companies to wage a psychological warfare embedded in fallacious statements in aim to undermine the importance of personal privacy, and prepare the collective psyche to accept a new status quo where privacy becomes a tale from the past. Most famously was the malicious statement made by former Google CEO, Eric Schmidt, when asked in a 2009 interview about whether Google should be trusted by users, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." (Esguerra) Around a month later, the CEO of Facebook (now Meta), Mark Zuckerberg made a similar statement, "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people," Mark continued, "That social norm [privacy] is just something that has evolved over time." (Johnson)

Conclusion:

Surveillance capitalism did not appear overnight, nor did it spring up from thin air. It was preceded by decades-long transgressions committed by the very authority that pledged to preserve the Constitution, serve American citizens, and protect their very rights it treaded on: the American government. This century-long violation of personal privacy has girded the loins for the American public's collective psyche to treat the continuing shrinkage of their civil liberties with a sense of indifference then eventually gave birth to something unknown, mysterious, and far worse.

Chapter Two:

The Function of

Surveillance Capitalism

Knowledge itself is power.

— Francis Bacon, *Sacred Meditations*, 1597.

The aim of knowledge [in the secular Western thought] is not to communicate with others, but to conquer them…. Therefore when [Francis] Bacon said that "Knowledge is [itself] power," he was establishing [the foundation of] the secular imperialist epistemology.

— Abdel Wahab El-Messiri, *Methodology of Dealing with Western Thought*, 1994

Introduction

The core of surveillance capitalism's business model relies on the extraction of personal data. This starting process operates in different forms, each to meet certain commercial objectives. And from its very beginning, surveillance capitalism has formed a highly profitable market that kept exponentially growing until it broke the barrier of twelve-figure annual revenues in recent years. So, how does this new market operate?

2.1. The Function of Surveillance Capitalism

2.1.1. Data Extraction

Technology companies claim that the sole purpose leading to the collection of data from their users and customers is to improve the overall quality of their services and products. While there is some truth to that, meaning that certain types of data at certain amounts are certainly needed to tweak and refine a service or a product, however, technology companies tend to extract extensively more data than they need for the aforementioned purposes. (Zuboff 70) As far as the legality of this operation, technology companies seem not to sway far from the law as they make sure that all the data extraction procedure is done under the consent of users and customers. How is that?

2.1.2 Terms, Conditions and Privacy Policy

To pave a road clear from any legal issues, tech corporations found a way to make users agree to anything they please: make terms, conditions and privacy policy exhaustingly long and full of vague legal terminology. These terms and conditions come as text in a dialogue box with a tiny checkbox on the bottom right that users have to check then click "agree" in order to ensure

that they consent with everything written above, and they cannot proceed to start using the website or the application if they don't.

Furthermore, an investigation carried out by the BBC found that privacy policy and terms and conditions on some well-known websites and applications were as long as novellas and plays and required a higher level of education to comprehend than the one needed to understand Charles Dickens's A Tale of Two Cities. Moreover, the word count of the privacy policy and terms and conditions concerning Facebook, WhatsApp, and YouTube, for instance, is nearing 7,000, and surpasses 10,000 for LinkedIn, Amazon, Apple, and Wikipedia, whereas it reaches 13,000 concerning Spotify, the world's largest music streaming service, which is nearly as long as Shakespeare's play Comedy of Errors, and takes 53 continuous minutes to read fully. (Calver and Miller) (See Figure 3)

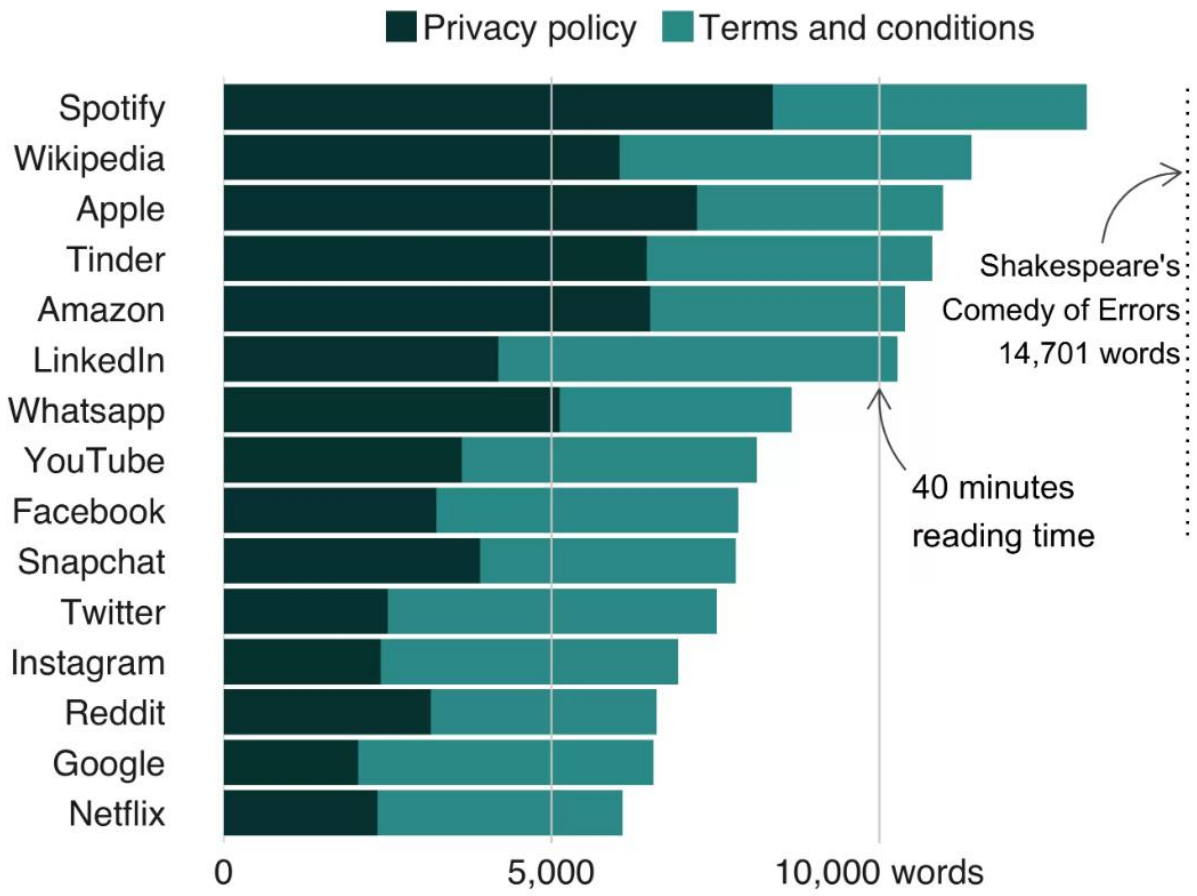
This psychologically well-crafted pitfall does exactly what it was meant to do: make the largest possible number of users abstain from reading what they are about to agree on and head directly to check the box and click "agree." This was proven overwhelmingly successful, as research conducted by the ProPrivacy website found that 99% of people do not bother reading terms and conditions. (Sandle) This means that almost every internet user unknowingly and, oddly, voluntarily permits every website, application, and service they use to collect, in a very short time, more information about them than the CIA, FBI, or any government intelligence apparatus would ever have. (Terms and Conditions May Apply 0:33:16)

And, as if things can't go worse, some companies and corporations allow themselves to change their privacy policy without notifying their customers and users, like what Facebook did in 2009 when the corporation secretly made changes in the privacy policy to grant itself more freedom in handling the data of its users. This, somehow, was exposed to the public resulting in an online

outrage followed by a formal threat by a consumer advocacy group coalition to pursue legal measures, which quickly forced Facebook to undo the changes. (Stone and Stelter)

Figure 3

Privacy Policy and Terms and Conditions' Word Count in the 15 Most Distinguished Websites and Applications



Source: BBC.com, "Social Site Terms Tougher than Dickens"

https://www.bbc.com/news/business-44599968

Correspondingly, the European Union, aiming at curbing Big Tech corporations, took a regulating action by adopting legislation called the General Data Protection Regulation, which

officially took effect on May 25, 2018. The GDPR's article 12 explicitly states that the way in which corporations and companies address their users and customers must be "concise, transparent, intelligible, and [in an] easily accessible form," the article continuous to emphasize that businesses are obliged to let their policies be known "using clear and plain language, in particular for an information addressed specifically to a child." By gaining the consent of their users and customers, technology companies are therefore guaranteed to work on legally safe ground and, thus, can extract any data type of data they included in the agreement. Moving on, the next step forward is to identify the variety of data extracted in this digital operation. ("Art. 12 GDPR")

2.1.3. The Four Classifications of User Data Collected by Technology Companies

Data that automatically generates as a result of humans' interaction with technology can be vast and encapsulates several aspects of the human experience if not all. However, technology companies classify that data into four categories.

2.1.3.1. Personal Data

Personal data is information gathered by technology companies, including, but not limited to, the Big Five: Google, Meta, Apple, Microsoft, and Amazon, which can be fairly described to be alarmingly extensive. Such information includes full name, age, sex, location, address, phone number, email address, IP address[4], browsing history, email messages, phone messages, financial information, online purchases, and face recognition data. (Chapman)

2.1.3.2. Attitudinal Data

[4] **IP Address**: A shortcut for Internet Protocol Address, IP address is distinctive set of dual and triple numbers divided by colons which gives electronic devices their unique identity.

It is the overall image a user or customer holds towards the company providing services or products. Attitudinal data can be collected in various ways; the easiest and most direct way is through text feedback and a five-star rating (rating the service or the product on a scale of one to five). (“How Companies Gather Data”)

2.1.3.3. Behavioral Data

Considered a mine of diamond in the market of surveillance capitalism as it represents the most precious and lucrative form of data to technology companies, behavioral data is data collected and then employed to have a profound understanding of users’ and customers’ personalities; it encompasses every minute detail of the way they interact online. Behavioral data can be the emails users and customers open and the ones they ignore, when they usually open them, the time they wake up, the time they go to bed, websites and pages they spend most of their online time engaging in, the hours, minutes and seconds they spend a day using a phone application, how many times they unlock their phones, social media posts and web articles they like, comment on, and share, and with whom they do, videos they watch, products they purchase online with the date and time they purchase them, and many other online behaviors that most consider either too insignificant or do not consider at all. (Wagner)

2.1.3.4. Engagement Data

It is data collected from the way users and customers engage with the companies’ advertisements on different outlets, and how they interact with emails and customer services. The main goal of collecting this data is to expand the reach of a certain product to a wider audience, and to understand what satisfies and frustrates the customer about a product or a service in order

to improve it, hence establishing strong customer retention[5]. ("How Companies Gather Data;" "How to Collect Engagement Data")

As mentioned earlier, behavioral data is the primary fuel by which surveillance capitalism operates; it is also the Kickstarter of what Zuboff calls the Behavioral Value Reinvestment Cycle. (Zuboff 70)

2.1.4. Behavioral Value Reinvestment Cycle

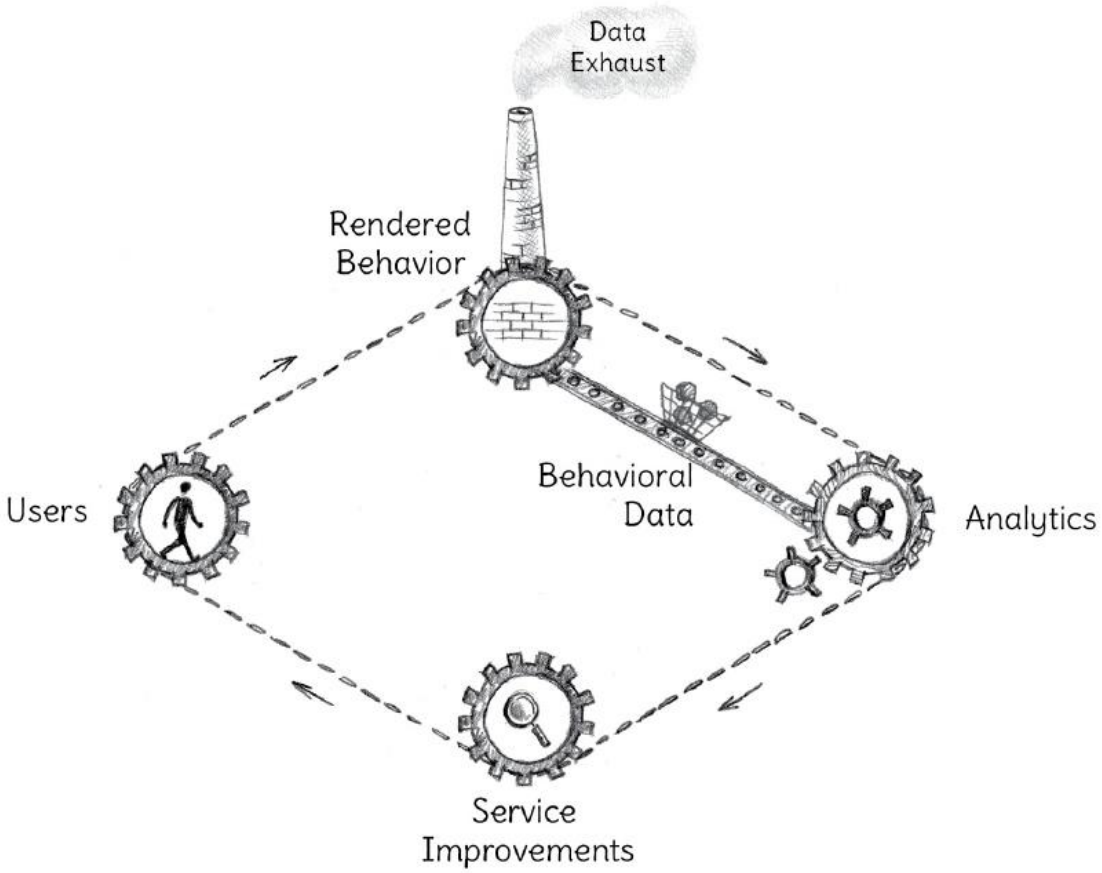
Primarily, the behavioral value reinvestment cycle is the process in which technology corporations keep collected quantities of data moving in an automated motion for the sole aim of service improvement. This cycle starts with the extraction of large quantities of behavioral data from users to undergo an advanced computational analysis. (Zuboff 70-71) In this step, behavioral data as a "value with no cost" is automatically fed to artificial intelligence models stored in large servers. These models are usually preprogrammed to learn from users and customers to expand the database of artificial intelligence, improve their computational potential, as well as to constantly keep up with the needs and wants of individuals on the other end. After behavioral data are fully digested and analyzed by artificial intelligence, the latter proceeds to improve services and products with high proficiency. This dual-ended process creates an interdependent win-win relationship between users and customers on one hand and artificial intelligence machines on the other. The rest of the accumulated behavioral data, which Zuboff refers to as Data Exhaust was deemed insignificant and marginal to the operation automatically discarded. (Zuboff 70-71) (See Figure 4)

[5] **Customer Retention:** The ability to transform regular customers into loyal ones.

This relatively innocent process of collecting people's personal data for the sole purpose of generating them into service and product refinement started as the initial business model of pioneer technology companies such as Google and Yahoo. And it was not so long until technology companies discovered that what they had thought to be data waste during the process of the behavioral value reinvestment cycle was, in fact, the underpinning of their new far more profit-making business model. (Zuboff 71)

Figure 4

Illustration of the Behavioral Value Reinvestment Cycle



Source: Zuboff, Shoshana, *The Age of Surveillance Capitalism*

2.1.5. From Data Exhaust to Behavioral Surplus

Certainly, the behavioral value reinvestment cycle as a business model was in the interest of users and customers; however, this interest was perceived by technology companies as unilateral, as investors' demands for a new lucrative business model started to get louder. For this matter, companies like Google wanted to attract more advertisers, but they also had to do so by presenting a more efficient advertising strategy. From this point, technology companies turned to their data exhaust, which became, as Zuboff defines, a behavioral surplus. This metamorphosis caused a tectonic change in the business model of technology companies and rendered the behavioral value reinvestment cycle, which was once limited and simple, into a small part that would trigger a larger and more intricate cycle. (Zuboff 75-76)

Technology companies started utilizing the behavioral surplus to tailor customized online advertisements in which they could target users and customers, individually or collectively, depending on several criteria. (Zuboff 76,79) Many, complex, and intertwined, the criterion with which technology companies target their users and customers can be classified as follows:

2.1.5.1. Demographic Targeting

Demographic targeting depends on basic information about users and customers that their family, friends, classmates, and co-workers are expected to know. This means that an individual is targeted here based on their sex, age, field of study, title of profession, and the like. In addition, demographic targeting has a flexible up-to-date ability to always keep up with what is happening in someone's life like family gatherings and friendly picnics, as well as what is going to happen, such as upcoming birthdays and other expected celebrations. (Planovsky)

2.1.5.2 Geographic Targeting

This type of targeting mainly depends on GPS[6] receivers embedded in technological devices like smartphones, tablets, and laptops. A device owner can easily turn off their GPS service, which can make some surmise they are untraceable in such cases. However, a device with turned-off GPS can still be tracked through various methods, one of which is by the constant signal transmission between the device and the nearest cell towers by which the exact location can be measured in an automatic operation that calculates the time it takes for signals to go back and forth. Another method of tracking is by public Wi-Fi; devices that have built-in Wi-Fi are constantly searching for access points whether the Wi-Fi is on or off. In this case, the location of someone passing by a group of public Wi-Fi, for instance, is determined through the strength of the signal of each access point captured by the device even if the latter is not connected to any of them. This means that it is almost impossible for people to hide their location while using an electronic device, which makes them prone to persistent geographic targeting. This means that it is almost impossible for people to hide their location while using an electronic device, which makes them prone to persistent geographic targeting. ("Can My Phone Be Tracked If Location Services Are Off?")

There is a wide variety of how geographic targeting can be used. For example, a company or a business owner can publish an advertisement that targets a specific country, region, or city, and they can also use a radius-based advertisement, meaning that a supermarket, for instance, can advertise their off-session discounts to everyone within the radius of 5 kilometers. (Planovsky)

[6] **GPS:** Stands for Global Positioning System, GPS is a technological service that provides precise location coordinates through satellites.

2.1.5.3. Platform Targeting

Here, advertisers get to choose what platform or website they can display their advertisement on for the aim of accurate collective targeting. For instance, if a company has a product or service that would interest people with ages ranging between 55 and 65, Facebook would be the perfect outlet in which they can place their advertisement. Sometimes, businesses can target a certain audience based on ideology and political orientation. How is that? Supposing that a business owner seeks to target an audience with a liberal inclination, they get to run their ads on known websites that hold the same beliefs; in this case, the New York Times, the Washington Post, NPR, and CNN would be the perfect choice. (Planovsky)

2.1.5.4. Interest Targeting

This type of targeting is based on a niche[7] an individual and their social circle are interested in. These interests can be discovered in various ways, like a search history of a person and their friends; for example, one can bump into an advertisement of a muscle gaining supplement either because they or one of their friends had searched for it earlier. Another way technology companies can determine what interests people is by eavesdropping through microphones built inside their devices. (Planovsky)

2.1.5.5. Keyword Targeting

Keyword targeting deals with very particularized terms people search for. For example, a real estate company would publish an online advertisement that would appear to anyone searching for "a 400 meters house in a safe neighborhood near an elementary school." (Planovsky)

[7] **Niche:** A job or a subject that perfectly fit with a person's interest.

2.1.5.6. Costume Audience Targeting

Although this type of targeting is not as far-reaching as the aforementioned ones, it has a unique advantage: create loyal customers by retargeting people who signed up to the business websites. For example, e-commerce companies like Amazon, eBay, and AliExpress would constantly retarget people who used their websites to buy or even to look for items by emailing them newsletters and discount offers. (Planovsky)

2.1.5.7. Third-Party Targeting

This type of targeting is based on data sold to an online advertising outlet (Facebook, Google, LinkedIn, etc) by a data broker, also known as a third-party provider. These data brokers, most notable of whom are Acxiom, Experian, and Epsilon, constitute an ever-rising data-broking market that tops $250 billion and is expected to reach $470 billion by 2032. (Vyas) Online advertising outlets resort to data brokers to be able to target, for instance, people with a certain social status who intend to buy a certain type of items of high value, such as a luxurious car, private jet, a mansion, or even a costly vacation trip. (Planovsky)

2.1.6. The Bigger Cycle

After swerving off the cycle of behavioral value reinvestment, data exhaust morph into behavioral surplus, which then undergo the process of assessment and analysis by potent and high-performing automated artificial intelligence. After analyzing the behavioral surplus, artificial intelligence not only can understand the behaviors of people, but it also can predict their future actions, needs, wants, cognitive changes, and even mental states. Whether a prediction about an individual would be precise only depends on the amount of behavioral data extracted from them and fed to the artificial intelligence of the technology companies. In general, there is a correlation

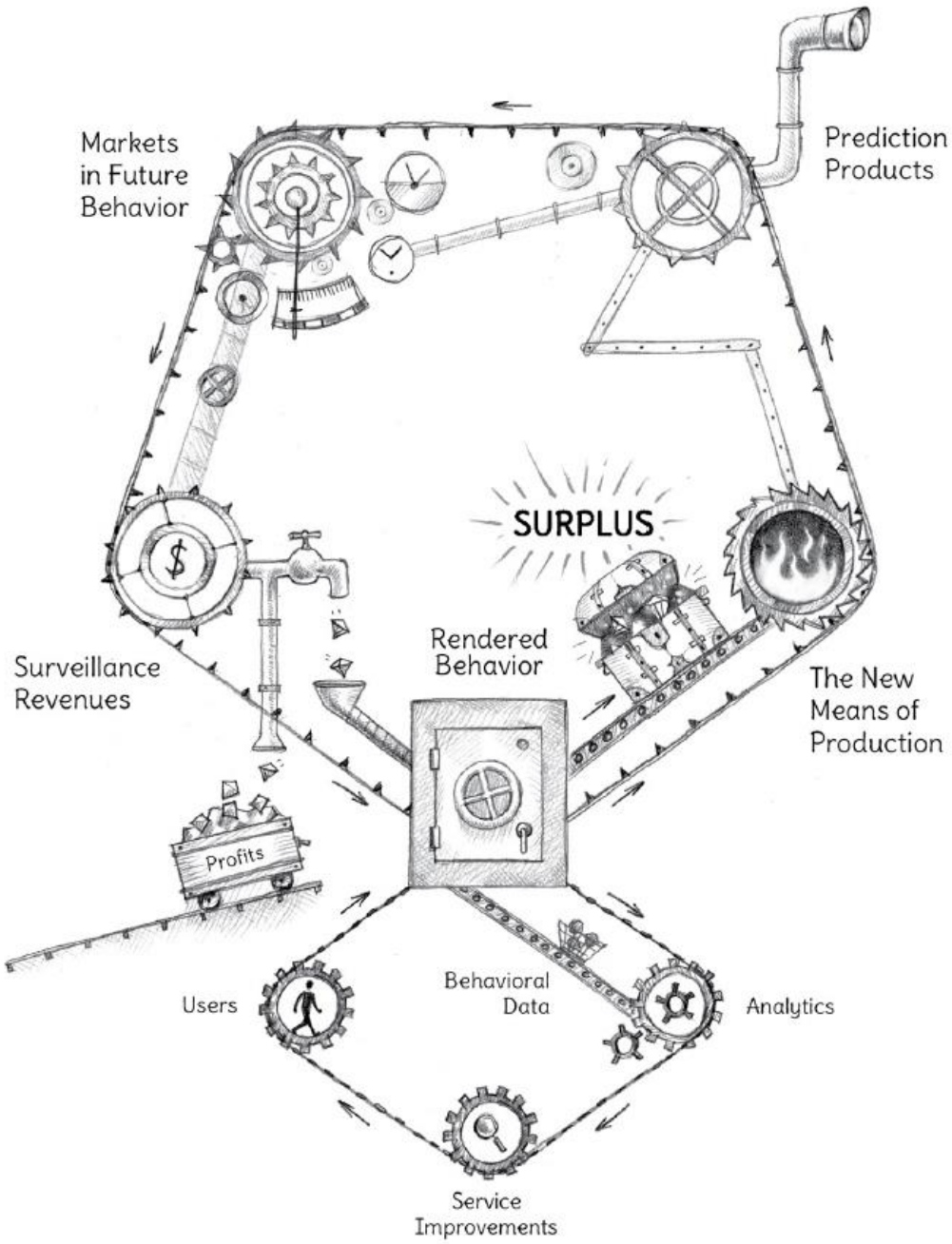
between the amount of the input and the efficiency of the output, meaning that the more quantity of collective behavioral data analyzed the more powerful the artificial intelligence becomes, thus, the better quality of reading people in the present and the future. (Zuboff 94-95)

To grasp the alarming nature of these prediction models, where are we standing now, the worrisome directions they may take, and the uses they may be subjected to, an incident that took place 12 years ago shall be a good eye-opener. Around a decade ago, the retail corporation Target created an artificial intelligence model to predict pregnancy. In 2012, which is a year later, a father in Minneapolis was constantly receiving coupons from Target that were meant for his teen daughter concerning baby clothes and cribs. It was only after he had contacted Target to complain, the daughter informed him that she was, in fact, pregnant. (Duhigg) This exceptional prediction of the pregnancy of a young female based on the vitamin and mineral supplements she had ordered should have the ability to illustrate a vivid perception of how dangerous these prediction models were, are, will become.

These types of precisions and predictions, which Zuboff refers to as "prediction products" are highly seducing for customers of surveillance capitalism, i.e., advertisers, who fully know that for every dollar they spend in these markets, the "behavioral futures markets," is worth spending. And as profitable as these markets are, thanks to their targeting capabilities, they have been expanding their services to offer more than advertising based on learning past and present behaviors to predict future ones but to modulate and alter people's behaviors, or even customize new ones. (Zuboff 95-96) (See Figure 5)

Figure 5

The Cycle of Surveillance Capitalism



Source: Zuboff, Shoshana, *The Age of Surveillance Capitalism*

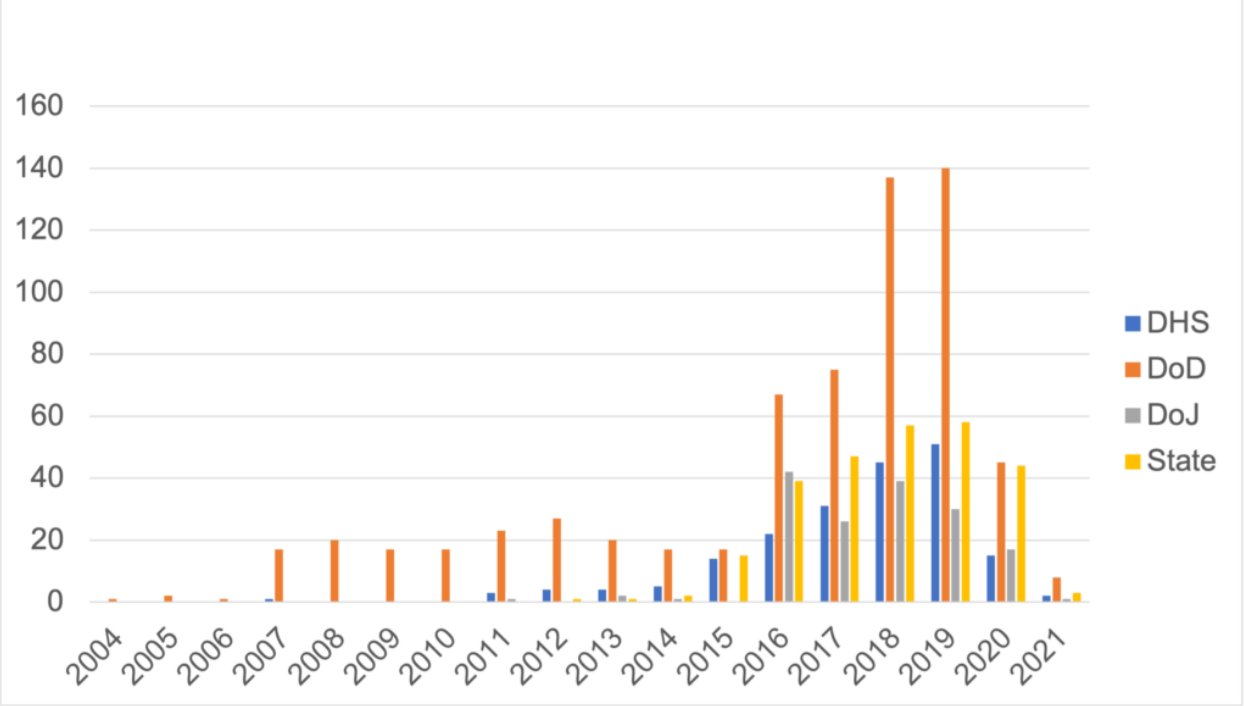
2.1.7. The Relationship Between the Private Sector and The Public Sector

The observer of the practices of the big technology corporation and their business model minions will, at some point, question the stance of the United States government on all of this. Well, the government of the United States has been deeply involved with data burglars in Silicon Valley[8], especially after the September 11 attacks. Led by the Department of Defense, the United States government agencies sought to invest in the evolving and far-reaching capabilities of technology corporations and companies for reasons ranging from assistance in the "war on terror" efforts and "preserving" homeland security, to upgrading law enforcement's monitorization abilities. Reports show that government agencies like the Department of Defense, the Department of Homeland Security, and the Department of Justice have been signing contracts and subcontracts[9] with top technology corporations since 2004, a period that witnessed a disastrous rise in violations of people's rights to privacy. Interestingly, the number of those deals kept gradually increasing until they started surging in the years 2015 and 2016 to reach an all-time high in 2019 when government agencies signed more than 340 agreements with Microsoft, Amazon, Google, Facebook, and X (previously known as Twitter) combined. Furthermore, it has been reported that the five aforementioned corporations had made more than $44 billion between 2004 and 2021 from deals with solely two government agencies: the Department of Defense and the Department of Homeland Security. ("Digital Destroyers") (See Figure 6 and Figure 7)

[8] **Silicon Valley:** A region in San Francisco, California where headquarters of the largest US technology companies are located.
[9] **Subcontracting:** When a company or an agency sign a commission with an individual, a group of individuals, or another company to do a certain job for them.

Figure 6

Total Number of Federal Contracts and Subcontracts with Amazon, Google, Microsoft, Facebook, and Twitter (X now) by Department

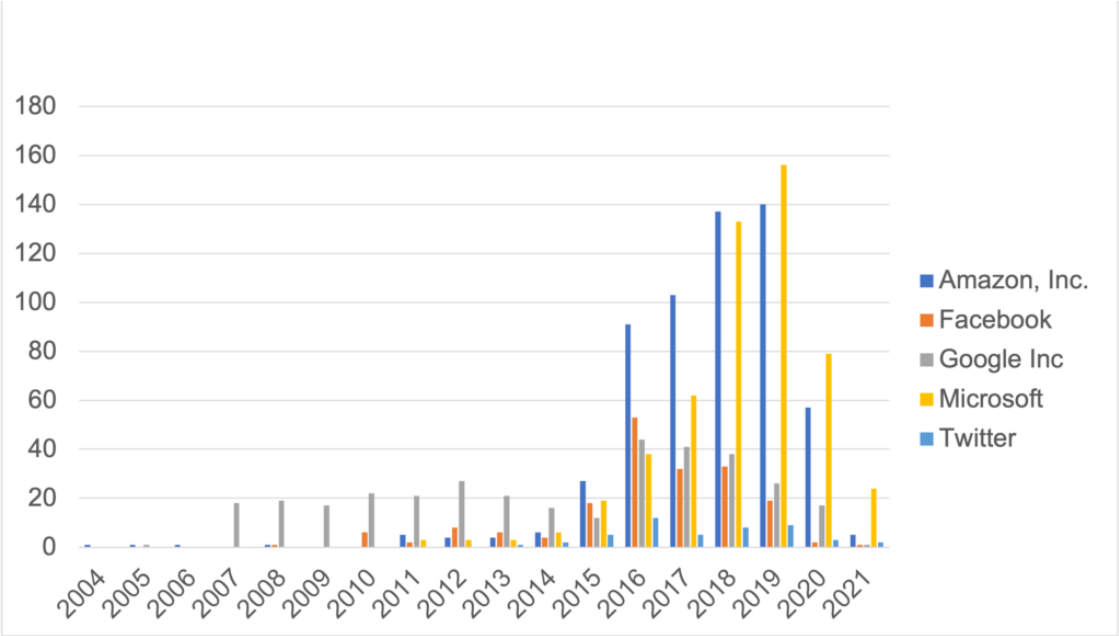


Source: Big Tech Sells War

https://bigtechsellswar.com/wp-content/uploads/2021/08/All-contracts-by-department-1024x636.png

Figure 7

Total Number of Government Contracts and Subcontracts Since 2004 by Technology Corporations



Source: Big Tech Sells War

https://bigtechsellswar.com/wp-content/uploads/2021/08/All-contracts-by-year-an-corp-1024x589.png

2.1.7.1. The Revolving Door

Noticeably, the primary reason for the smooth cooperation; the increasing number of deals; and, in general, the ever-stable state of affinity between the United States' government and giant technology corporations is the strong influence of lobbying personnel deeply embedded within government agencies, including their executive arms, such as the Department of Defense's

National Security Agency (NSA) and The Department of Justice's FBI. Big technology corporations get to maintain this state by turning high-ranking officials in the public sector into lobbyists with two main missions: Preventing regulations that could harm the corporations and advocating for policies that could either grant the corporations new spaces of freedom or lock high-profit deals between the latter and government agencies. In return, lobbyists will be guaranteed important positions in the technology corporations for the future. This process of moving from the public sector to the private sector is known as the revolving door. (González; Khanal et al.)

There have been many detectable instances of revolving door activities concerning technology corporations in the stretch of the last two decades. One of the prominent cases is Sheryl Sandberg. Sandberg worked as the Chief of Staff under the United States Treasury Secretary Larry Summers from 1999 to 2001; the year in which she started working for the back-then newly-born small start-up with no more than 300 employees Google. She was appointed as the general manager of the business unit; a unit specialized in Google's advertising program. Sandberg's adventure in Silicon Valley witnessed a switch when she joined Facebook (Meta) in 2008 as a Chief Operating Officer (Hartmans and Nolan) Sheryl Sandberg has made a vital contribution to the creation of surveillance capitalism and its current operating business model due to her role in developing and expanding Google and Facebook, which are considered to be the two main designers of surveillance capitalism. (Zuboff 91-92) In 2023, the former United States Treasury Secretary and Sandberg's former boss, Larry Summers, became one of the three board members of the world-leading Artificial Intelligence research organization OpenAI. (Salmon) Disturbingly enough, Sheryl Sandberg and Larry Summers are only two examples of countless others who passed through the revolving doors. ("Digital Destroyers")

Conclusion:

Surveillance capitalism is an impressive, complex, and fine-tuned market. This market functions through the basis of tyranny and totalitarianism where there is no such thing as personal privacy where every piece of information belongs to the Silicon Valley. Constituents of this market take advantage of people's need for convenience to plunder their personal data which encapsulates who they are for the purpose of gaining multi-billion revenues. And there are little to no laws that can effectively regulate this market and curb its threats to civil liberty thanks to coalition lobbyists inside the decision-making rooms.

Chapter Three:

Cambridge Analytica's Involvement in the United States' 2016 Presidential Elections

The greatness of man is not primarily in the doing of good deeds but in his ability to choose.

— Alija Izetbegović, *Islam Between East and West*, 1980.

Introduction

As briefly mentioned in Chapter Two, the extraction and analysis of behavioral data to target individuals and populations with high-precision advertisements was not the terminal of surveillance capitalism's railway, as giant technology corporations' ambitions seem to have no limits, especially with the destined absence of deterring regulations thanks to the powerful influence of lobbyists. Technology corporations took a further step, a way further one, by beginning to implement behavioral to data modify people's behaviors in order to achieve their own political, social, cultural, and above all, commercial ends. So, how can technology corporations modify behaviors, and to what extent can they do so?

3.1. Cambridge Analytica's Backstory

Cambridge Analytica was a data-driven consulting firm created in 2013 as a subsidiary of the Strategic Communication Laboratories, also known as SCL Group, a political multi-service British company. It was mainly specialized in running online political campaigns inside and outside the United States. (Fernando)

Before Cambridge Analytica's creation, its parent company had been involved in political campaigns in 32 countries across five continents, preeminently, Argentina, Colombia, Italy, Ukraine, Nigeria, South Africa, India, Indonesia, and several more. (Ghoshal) In 2016, Cambridge Analytica was appointed by the United Kingdom Independence Party to carry through their controversial *Leave.EU* campaign, also known as Brexit, was a political movement that succeeded later that year and led the United Kingdom to split away from the European Union through what was known as 2016 United Kingdom European Union Membership Referendum. (Scott) Eventually, the firm filed for bankruptcy and was terminated in 2018 after news broke out

concerning their scandalous set of misconducts during their campaign for the back-then Republican candidate Donald Trump in the 2016 United States Presidential Elections. (Watkins)

3.2. Cambridge Analytica's Involvement in the 2016 U.S. Presidential Elections

The 2016 United States Presidential Elections were highly controversial, as they witnessed a major twist that resulted in an unexpected outcome: Donald J. Trump, the new resident of the White House. Throughout the set of months leading up to election day, the overwhelming majority of conducted polls showed an undisputed leading by the back-then Democrat candidate Hillary Clinton with a total average of 45.7% versus 41.8% for Donald Trump on the other hand, ("National Polls") while election forecasting[10] showed a tremendous 71.4% chance of winning for the Democrat candidate versus 28.6% for the Republican candidate. ("Who Will Win the Presidency?") Some evidences suggest that this sway of events could be the result of Cambridge Analytica's fraudulent intervention in the scene. (Auchard and Ingram) The question is, how could they do it?

3.2.1. The Four Horsemen of the Trump Campaign

Several individuals, whether from Trump's side or Cambridge Analytica's, were involved in the 2016 campaign, but only four of them were the prominent key players: Robert Mercer, Steve Bannon, Alexander Nix, and Aleksandr Kogan. (Cadwallad and Graham-Harrison)

3.2.1.1. Robert Mercer

[10] **Election Forecasting:** Model built on certain circumstances and events with the objective of predicting elections' results.

An artificial intelligence scientist and a billionaire, Robert Mercer was one of the biggest donors to the 2016 Trump campaign with over $25 million. (Boag) Mercer was also the owner and the funder of Cambridge Analytica. (Cadwallad and Graham-Harrison)

3.2.1.2 Steve Bannon

Steve Bannon is a political consultant, a filmmaker, and a former executive chairman of the ultra-right-wing media website Breitbart. Thanks to his close relationship with the Mercer Family, Bannon, who had been the vice president of Cambridge Analytica, talked Robert into funding the company by convincing him of its project. Robert then recommended him to Donald Trump to head his campaign; this led Trump to name Bannon as the chief executor of his 2016 presidential campaign. After winning the presidency, Trump appointed Bannon as the White House's chief strategist. (Boag; "Steve Bannon,")

3.2.1.3. Alexander Nix

Alexander Nix is a British entrepreneur and the former chief executive officer of both SCL Elections, the parent company of SCL Group and Cambridge Analytica, and the British branch of Cambridge Analytica. Thanks to Robert Mercer's investments, Nix was able to establish a new branch of Cambridge Analytica in the United States. (Cadwallad and Graham-Harrison)

3.2.1.4. Aleksandr Kogan

Aleksandr Kogan is Moldovan-American who worked as an associate professor in Cambridge University where he lectured on psychology and social media psychometrics[11].

[11] **Psychometric Profiling:** The process of gathering data about an individual in order to build a precise psychological profile about him or her.

(Cadwallad and Graham-Harrison) In 2014, Kogan founded a data research start-up company in the United Kingdom called Global Science Research, briefly known as GSR. (Wong et al.)

3.2.2. Cambridge Analytica at Work

The following will articulate the framework by which Cambridge Analytica operated during Trump's 2016 presidential campaign.

3.2.2.1. Global Science Research Harvests the Data

At the outset of their journey to get Donald Trump elected for the presidency, Cambridge Analytica, who had been in business cooperation with Global Science Research since 2014, granted Aleksandr Kogan $1 million in request to harvest data through his research company. (Cadwalladr) Kogan then created an innocuous-looking fun app called This is Your Digital Life where people can take a personality test by inputting certain types of personal information and getting paid less than $5 in return. The key move here was that users had to sign up for the quiz app through their Facebook accounts (Hern; Ingram); this would automatically direct them to the Request for Permission section where they would be asked to grant the app permission to access their information, which includes a list of friends and any information shared with others. (Hartmans) Within a few weeks after its launch, more than 270,000 people had downloaded This is Your Digital Life, and thanks to their unsuspecting consent, the app harvested the participants' personal and behavioral data and merged them with the results of their survey answers to create a psychometric profile for every single user. Additionally, the app harvested the personal and behavioral data of all of the participants' friends as well. This gave Aleksandr Kogan's Global Science Research access to around 87 million Americans' critical data, which led

them next to acquire their voting records. (Chang; “How Cambridge Analytica Exploited the Facebook Data of Millions” 0:00:58)

3.2.2.2. Voting Records

Voting records are registered sets of archived information concerning citizens who practice their right to vote. Some of these pieces of information can be sensitive and may also be considered highly valuable by corporations and companies that constitute the market of surveillance capitalism. Some information within voting records like names, home addresses, and political affiliations are publicly available; however, other detailed and thorough pieces of information can only be obtained through submitting an official written request by a limited number of parties and individuals. These include government officials, law enforcement, political parties, candidates, journalists, and scholars, which is probably how Dr. Aleksandr Kogan, a scholar himself, got his hands on the voting records of the floods of people whose online data were already harvested. (Williams) The full personal information found in voting records is as follows:

Table 1

Personal Information Contained in Voting Records in the United States

Voting Record Information	Examples
Identifying information	• Date of birth • Gender • Father's name or mother's maiden name • Social Security number • Military ID • Passport number • Driver's license number • State identification card
Address information	• Home address • Mailing address • Voting district • Polling Place
Contact information	• Phone number • Email address
Voting information	• Party affiliation • Absentee ballot • Precincts, registering agency, or required assistance • Last voting date, e.g., local election or primary election
Miscellaneous information	• Prior felony conviction • Last date of jury duty • Active or inactive voter registration status • Date when information was last updated

Source: Findlaw.com

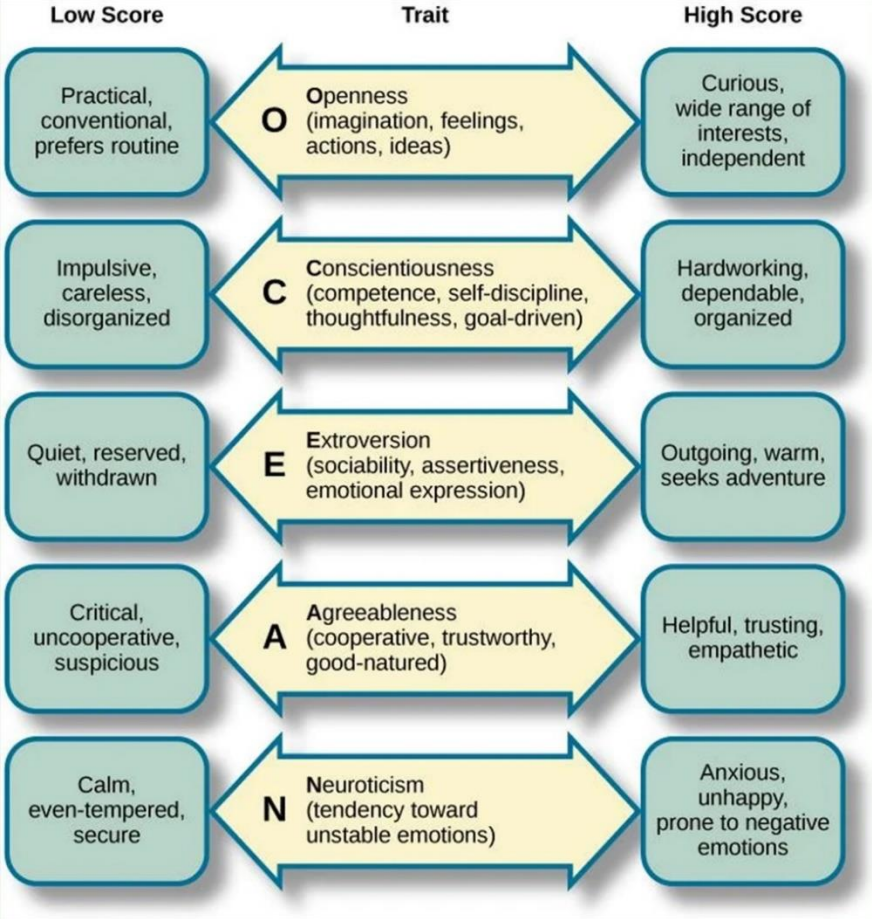
https://www.findlaw.com/voting/how-u-s--elections-work/what-information-is-public-from-your-voting-record.html

3.2.2.3. Cambridge Analytica's OCEAN

Dr. Kogan sent the data his company had accumulated and stored to Cambridge Analytica, who in turn put them under advanced psychological classification scientifically referred to as *OCEAN*, (Hern) which is based on a theory speculated by American psychologist D.W. Fiske in 1949 then developed by several scholars over the following decades. The theory suggests that among all personality traits that humans have, there are five underpinning ones by which an individual's personality can be assessed: openness, conscientiousness, extroversion, agreeableness, and neuroticism. The theory assesses individuals' overall personalities by measuring the extent to which they incline toward each of the five traits. (Darby) (See Figure 8)

Figure 8

How the Score of the Five Personality Traits Can Shape the Personality



Source:SimplyPsychology.org

https://www.simplypsychology.org/big-five-personality.html

3.2.2.4. Psychographic Microtargeting

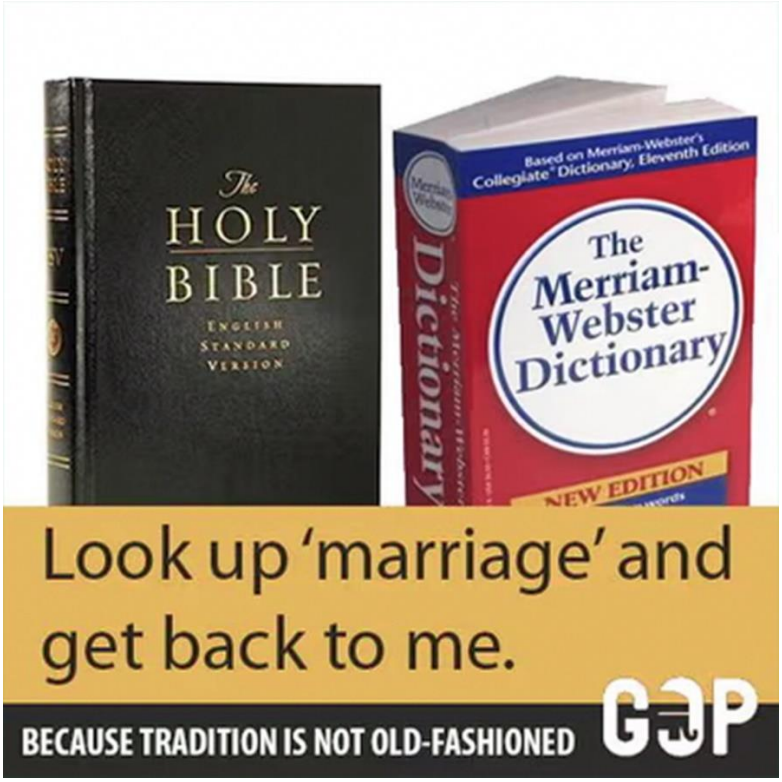
Equipped with a colossal amount of their sensitive data, Cambridge Analytica analyzed each voter's profile individually using state-of-the-art artificial intelligence algorithms to in aim

to single out each voter with a dog-whistle type of political advertising, meaning that each voter would be exposed to a piece of propaganda crafted especially for him or her. (Hern) This is known as psychographic microtargeting where each individual is targeted with a high psychological precision based on their OCEAN assessment results in order to nudge them into adopting certain perspectives and behaviors by exploiting their inner fears and motives. (Resnick)

Concerning Donald Trump's 2016 presidential campaign, numerous instances of psychographic microtargeting can be found in the archives; however, inspecting a couple of them would be enough to formulate clear insight. The first example was one out of many uniformly-graphically-designed billboards: an image with a bible next to a dictionary book with a short sentence underneath, "Look up 'marriage and get back to me." Obviously, this advertisement was designed to target those who value the institution of conventional marriage and family and oppose the liberal and ultra-liberal agendas that advocate same-sex marriage. A former Cambridge Analytica employee commented on this particular image by explaining that "It was targeting conscientious people." The former employee carried on elaborating, "For someone who is conscientious, it is a compelling message: a dictionary is a source of order, and a conscientious person is more deferential to structure." (Hern) (See Figure 9)

Figure 9

A Sample of Cambridge Analytica's Psychographic Microtargeting Advertisement



Source: The Guardian.com

https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

3.2.2.5. Persuasion Search Advertising

The second example falls within a subcategory of psychographic microtargeting called persuasion search advertising where internet users are targeted with links that appear on the very top of their search results based on their search queries. During the 2016 presidential campaigning,

internet users in the United States ran across several persuasion search advertising as they surfed online; for example, those who wanted to know Trump's stance regarding the country's involvement in foreign wars and typed a query with the three algorithmic triggering keywords "Trump, Iraq, War" were immediately targeted with a top result link with well-designed concluding titles suggesting two contrasting pieces of information, one to intimidate and one to encourage: Hillary Clinton is a warmonger; Donald Trump is a pacifist. (Lewis and Hilder) (See Figure 10)

Figure 10

A Sample of Cambridge Analytica's Persuasion Search Advertising

Source: The Guardian

https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory

3.2.2.6. Elitism Propaganda

Fundamentally, elitism propaganda is a more prestigious way of name-dropping, where a person who seeks to climb the social class ladder starts mentioning their association with other individuals who are often more famous, popular, and powerful. Politicians, too, use this tactic in order to seal certain objectives ranging from reaching a political position to acquiring actual or psychological immunity from jurisdiction. (Mangwana)

Cambridge Analytica used this promotion technique chiefly to target voters in swing states[12] with the help of their already-harvested geographical data. Usually, swing states tend to contain a great deal of ambivalent voters; those who cannot seem to have made up their minds and stick with one candidate throughout the whole campaign up to election day. The consultant company designed billboards and displayed them on several leading websites online where they tried to convince swing voters that Donald Trump had the endorsement of many well-known celebrities in various classes and domains. The billboards would show a row of famous and popular individuals: A successful businesswoman (Trump's daughter) to attract female voters; a television personality coming from a middle-class background to attract middle-class voters; a strict law-enforcing black sheriff to kill two birds with one stone: first, to attract African-American swing voters; second, to attract those who are high on the conscientiousness and neuroticism scale and want the country to be ruled by those who are strong enough to force law and order; a retired navy

[12] **Swing States:** The States that are not consistent in their presidential election choices where voters constantly swing between Democrat and Republican candidates.

seal to attract veteran swing voters; and the president of the Ultimate Fighting Championship to attract athletes and young swing voters. (Lewis and Hilder) (See Figure 11)

Figure 11

A Sample of Cambridge Analytica's Online Billboards

Source: Theguardian.com

https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory

3.3. The Effect of Cambridge Analytica on the 2016 United States Presidential Elections

Several political scholars and commentators seem to undermine Cambridge Analytica's role in the 2016 Presidential Elections in the United States as they claim that swaying voters' beliefs, let alone behaviors, would require much more than mere online advertisements here and there. (McNeil) Skeptics argue that the utmost technology corporations and companies can do would be no farther than nourishing voters' preformed biases. (Resnick) However, the overstating denial of surveillance capitalism's real capabilities shall evoke our suspicions and curiosity and lead us to take a relatively uncharted road to decipher the factual effect of Cambridge Analytica. Saying so, and in order to gauge the extent to which the consulting company affected the

presidential elections, several principal aspects of the equation ought to be initially considered, first of which: How does the United States' presidential election work?

3.3.1. The Electoral College

Unlike all other countries where the president is the one who wins the majority of votes countrywide, the presidential election system in the United States is based on what is known as the Electoral College. It is a method where the candidate who wins the majority popular votes statewide automatically seals the total votes of electors, which are people appointed by their parties to reflect, in most cases, the popular votes within each state into their electoral votes. This is true to 48 states except two: Maine and Nebraska where the candidate who wins the majority of votes in the state takes two electoral votes and the rest of the votes individually go to the one who wins the majority of votes within the congressional districts, meaning that a candidate takes one electoral vote for each congressional districts they win the popular votes of. Nebraska has three congressional districts, therefore three electoral votes, whereas Maine has two. (Ray; "Split Electoral Votes in Maine and Nebraska")

Moreover, each state has a different number of electors. For example, the State of California has 54 electoral votes, which is the highest; the State of Texas has 40; and the State of South Carolina has 9. This distribution of electoral votes creates a reality where some states are more important and decisive than others. ("Distribution of Electoral Votes") Moreover, in contrast to swing states, some states have a persistent historical record of voting for one certain party in each presidential election. For instance, the popular votes in the State of Texas went to the Republican candidate in every presidential election since 1980, ("Texas") In contrast, the State of California has been siding with the Democratic candidate since 1992. ("California,") In general, the candidate who wins at least 270 electoral votes becomes president of the country. (Ray)

3.3.2. Cambridge Analytica's Effect on the Election

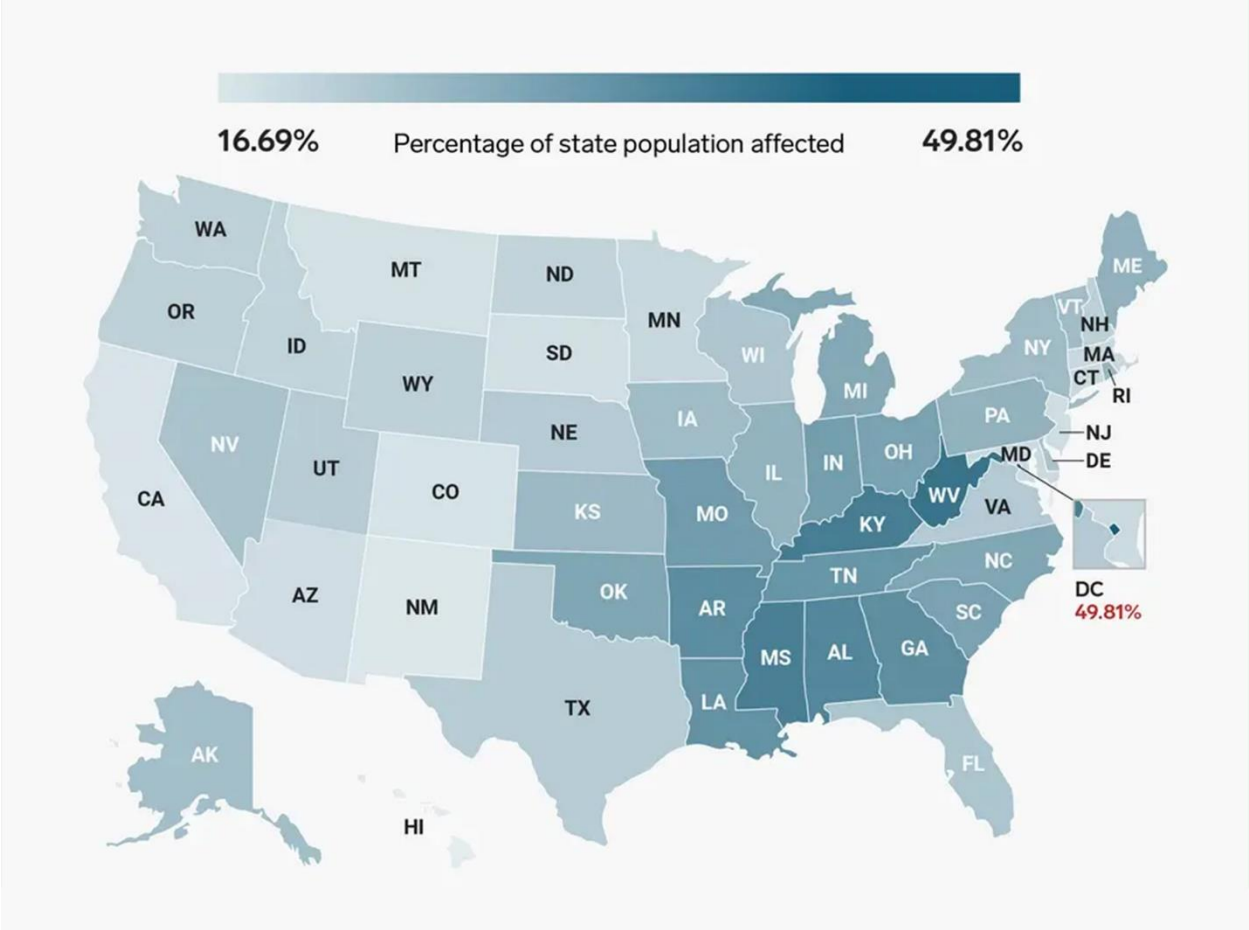
Statistical data show that Cambridge Analytica conducted different types of targeting on all American states, but the intensity varied from one state to another. In addition, it is discernible that the consultant company knew exactly what they were doing as they conducted their job in a well-measured manner. For instance, Cambridge Analytica exploited the fact that Hillary Clinton had neglected the Rustbelt[13] states as the former First Lady thought she had the highly important region in her pocket and took it for granted, which made her have little to no campaign there. (Bhardwaj and Lee; Brownstein)

The apparent and potential reason for that seems to be her fellow Democratic and former President Obama's impressive performance in these states in both 2008 and 2012 where he triumphed in all of the Rustbelt states except for Missouri and Indiana in 2012. ("New York;" "Pennsylvania;" "Ohio;" "Michigan;" "Wisconsin;" "Iowa;" "Illinois;" "Missouri;" "Indiana;") Cambridge Analytica targeted these states in a relatively high concentration as well as Florida and North Carolina where Clinton heavily campaigned. (Bhardwaj and Lee; Brownstein) On the other hand, some states were scantily covered with any operations, whether because they were historically rigid Democratic states like Washington D.C., Oregon, California, Colorado, and New Mexico, or due to the total opposite, like Montana and South Dakota, so targeting them would have been costly with no value in return. (Bhardwaj and Lee; "Washington;" "Oregon;" "California;" "Colorado;" "New Mexico;" "Montana;" "South Dakota") (See Figure 12)

[13] **Rustbelt:** The Rustbelt is the geographical region covering New York, Pennsylvania, Ohio, Michigan, Wisconsin, Indiana, Missouri, Iowa, and Illinois, which once was thriving with industrial manufactories and coal and steel mines that were abandoned later.

Figure 12

Map of State Populations Targeted by Cambridge Analytica



Source: Business Insider

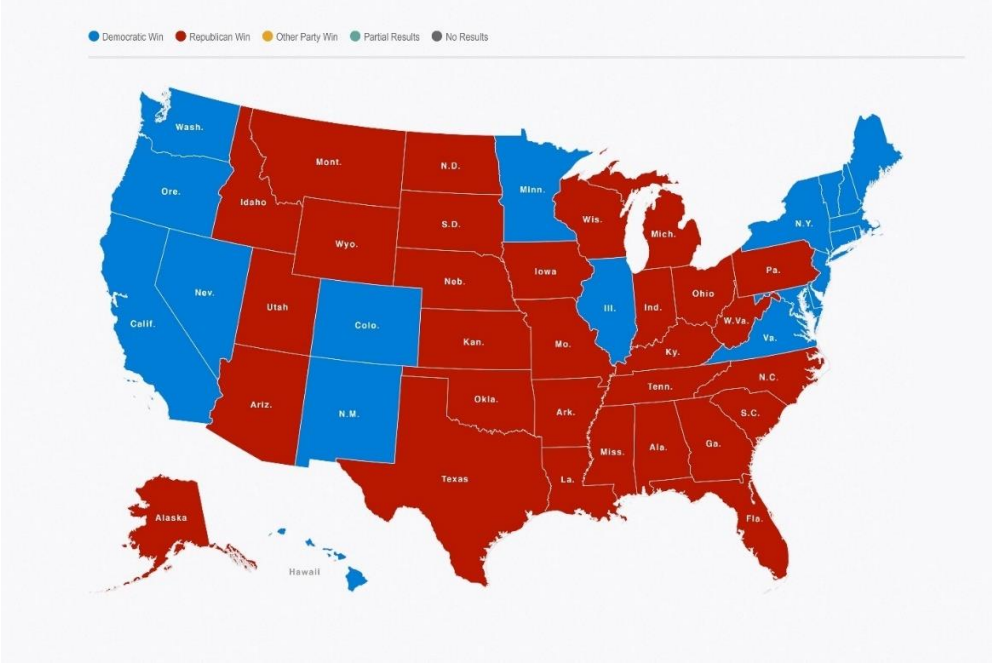
https://www.businessinsider.com/facebook-cambridge-analytica-affected-us-states-graphic-2018-6

Ultimately, the results of the elections show an unmistakable pattern that demonstrates the level of Cambridge Analytica's effectiveness: Donald J. Trump was elected as president after

collecting 306 electoral votes with an overwhelming 91 votes from the Rustbelt states where the newly elected president won in all states of the region except for New York and Illinois. Besides, Trump won in Florida and North Carolina, which are crucial swing states, and gained an additional 44 electoral votes (135 electoral votes in total). And although some discrepancy can be noticed in the pattern where Hillary Clinton won in several states where Cambridge Analytica allocated a remarkable deal of focus such as the States of Maine, New Hampshire, Vermont, New York, Massachusetts, Rhode Island, Delaware, Illinois (77 electoral votes in total), still, the success of the Trump's consultant company in certain vital states greatly outweighs their failure in others that, mostly, have less electoral votes, which deems them less important. . (Bhardwaj and Lee; "2016 Presidential Election Results,") (See Figure 13)

Figure 13

Map of the 2016 Presidential Election Results



Source: Politico.com

https://www.politico.com/2016-election/results/map/president/

All of the aforementioned do not conceal the reality that other factors played a role in the outcomes of the United States 2016 Presidential Elections, primarily the big scandal when Wikileaks gradually disclosed to the public over 30,000 Hillary Clinton private emails during the few weeks leading up to the Elections, which revealed devastating misconducts that detrimentally affected her image. (Enten; Gerstein)

Conclusion:

Cambridge Analytica used its pioneering experience to carry out its job as a consultant for Donald Trump's campaign through unlawful and unethical means. Demonstrated data show that the firm had performed a nationwide series of propaganda campaigns that targeted almost half of the American voter population. Overlapping that data with the results of the United States' election reveals a clear pattern that leads to one conclusion: Cambridge Analytica had a major impact on the outcome that granted Donald Trump the chair of the Oval Office desk.

General Conclusion

This research sought to backtrack the historical periods and events that paved the way for surveillance capitalism to develop. This research also aimed to demonstrate the system by which the market of surveillance capitalism operates, how giant technology corporations use open legal interpretations and loopholes to infringe the constitutionally protected citizens' right to privacy and harvest their data, and the complicated cycle through which data undergoes to generate multi-billion revenues. Additionally, this research took Cambridge Analytica as a microcosmic sample of surveillance capitalism and explored its business model, footprints, and illegal and unethical misconduct while campaigning for Donald Trump in his 2016 presidential campaign.

Based on this research, surveillance capitalism can be defined as an authoritarian relationship based on unbalanced reciprocity through which technology companies force people to consent to the looting of their private data in return for convenience. In this relationship, people get to use services and technology companies get to generate multi-billion revenues, and more, deepen their understanding of individuals' needs, intellectual inclinations, and psychological strengths and weaknesses, and alter their behavior in ways that meet their needs. Based on this observation, it is safe to say, with no exaggeration, that surveillance capitalism can be classified as the worst manifestation of capitalism. It ironically embodies what a regular American citizen thought of communism during the highest peak in the Cold War. It is the manifestation of capitalism under which the most basic and humane ethics and values were degraded.

Data presented and analyzed in this research indicates that the market of surveillance capitalism has been enlarging at an exponential pace over the recent years, which resulted in the market's increase of influence that interwoven deep into the political, economic, and social fabric of the United States and the world in general. This increasing influence poses a dangerous threat to the two essential pillars of freedom: the right to undisturbed personal privacy and the right to

intellectual autonomy. Moreover, data presented in this research show that the mechanism in which surveillance capitalism functions is so potent that a relatively small company like Cambridge Analytica was able to influence the presidential election result of what the world considers the beacon of democracy, the United States of America. This raises the alarm to the fact that democracy around the world can be facing an existential, especially in this age where people, to a great extent, have abandoned conventional means of information exposure and started taking outlets owned by surveillance capitalists as their main source of information.

Furthermore, data presented in this research show the solid and intertwined relationship between the constituents of surveillance capitalism and lawmaking constitutions in the United States. The obscure line that connects the two ends of the relationship is lobbying, through which high-ranking government officials switch between the public and the private sector in a constant manner to pursue personal ambitions. This operation guarantees to preserve the no-regulations status quo for giant technology corporations where they are exempt from any legal development that would disturb the market of surveillance capitalism.

This study was conducted, to a considerable extent, with the help of data leaked by whistleblowers who once worked inside the market of surveillance capitalism. Other data on surveillance capitalism are shallow and superfluous and have little to no real value that can help enrich the literature on this subject matter. This reveals the level of secrecy under which this market operates. It also suggests that there is, certainly, more than meets the eye as further data needs to be put in the hands of the public so a wider and clearer image about the market of surveillance can be illustrated.

This study reveals that there is a serious equation that rules this digital age which every individual must take into consideration: the more convenient the technology the more personal

privacy is compromised. This means it is true that the technology devices we use today, such as smartphones, computers, and smartwatches, do make our life easier, but it is a comfort that comes at the heavy expense of what makes us who we are; our very privacy. This findings in this study show the grave need for people to value their privacy and work more on conserving it even if they think they have nothing to conceal. In addition, more people need to raise their voices and expose surveillance capitalism and its constituents so a public pressure strong enough can be generated to force governments across the world to take the right actions. Finally, studies tackling surveillance capitalism, the way it functions, and its effects are scarce and limited. This calls for further research to be conducted on this matter.

Works Cited

Books:

Friedman, Milton. Tyranny of the Status Quo. 3rd ed., Houghton Mifflin Harcourt, 1984. p. 115.

Véliz, Carissa. Privacy Is Power. 1st ed., Bantam Press, 2020. pp. 36-38.

Cappello, Lawrence. None of Your Damn Business: Privacy in the United States from the Gilded Age to the Digital Age. 1st ed., The University of Chicago Press, 2019, https://doi.org/DOI: https://doi.org/10.7208/chicago/9780226557885.001.0001. pp. 77-78.

Price, David H. The American Surveillance State. 1st ed., Pluto Press, 2021. p. 34.

Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. 1st ed., Public Affairs, 2018. pp. 70-92.

Izetbegović, Alija. Islam Between East and West. 1st ed., The American Trust Publications, 1980. p. 115

Bacon, Francis. Sacred Meditations. 1595.

Articles and Websites:

Richards, Neil M. “The Dangers of Surveillance.” Harvard Law Review, vol. 126, no. 7, May 2013, pp. 1934–1965, www.jstor.org/stable/23415062.

Foster, John B., and Robert W. McChesney. “Surveillance Capitalism.” Monthly Review, 1 Jul. 2014. https://monthlyreview.org/2014/07/01/surveillance-capitalism/*

Zuboff, Shoshana. “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization.” Sage Journals, vol. 30, no. 01, 2014, pp. 75-89, https://journals.sagepub.com/doi/10.1057/jit.2015.5. Accessed 5 Sept. 2024.

Conolly-Smith, Peter. “”Reading Between the Lines”: The Bureau of Investigation, the United States Post Office, and Domestic Surveillance During World War I.” Social Justice, vol. 36, no. 01, 2009, pp. 7-24, https://www.jstor.org/stable/29768523https://www.jstor.org/stable/29768523. Accessed 19 Jul. 2023.

History.com Editors. “FBI Founded.” HISTORY, 22 Feb. 2019, www.history.com/this-day-in-history/fbi-founded.

“The Full Text of The Mann Act.” PBS, www.pbs.org/kenburns/unforgivable-blackness/mann-act-full-text. Accessed 19 Jul. 2023.

“Black Tom Island Explodes.” Intellegence.Gov, www.intelligence.gov/evolution-of-espionage/world-war-1/sabotage-subterfuge-and-war/black-tom-island-explodes. Accessed 20 Jul. 2023.

Tagg, Lori. “February 1918: WWI Counterintelligence Agents Get Their Man.” Army.Mil, 10 Feb. 2017, www.army.mil/article/182075/february_1918_wwi_counterintelligence_agents_get_their_man. Accessed 20 Jul. 2023.

“The Espionage Act of 1917.” Digital History, www.digitalhistory.uh.edu/disp_textbook.cfm?smtID=3&psid=3904. Accessed 20 Jul. 2023.

"Title 50 - Appendix-War and National Defense Trading with The Enemy Act of 1917." Justia Law, law.justia.com/codes/us/2010/title50/app/tradingwi/sec19. Accessed 21 Jul. 2023.

Mitchell, C. "What is a Conviction Rate?" My Law Question, 16 May 2024, www.mylawquestions.com/what-is-a-conviction-rate.htm. Accessed 8 Aug. 2024.

"Dictaphone." Collins Dictionary, www.collinsdictionary.com/dictionary/english/dictaphone. Accessed 10 Aug. 2023.

"Sedition Act of 1918." U.S. History, www.u-s-history.com/pages/h1345.html. Accessed 10 Aug. 2023.

Morgan, Ashley E. "Government Surveillance and The War On Terror: Why Is Government Cyber Data Collection Increasingly Sanctioned by the Courts, Despite The Development of Privacy Law Protections Against Domestic Surveillance Beginning in the Early Twentieth Century?" Seton Hall ERepository, 2019, p. 4, https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1952&context=student_scholarship. Accessed 11 Aug. 2023.

"Olmstead V. United States (1928)." Constitution Center, constitutioncenter.org/the-constitution/supreme-court-case-library/olmstead-v-united-states. Accessed 15 Aug. 2023.

"Establishment of the CIA." Truman Library, www.trumanlibrary.gov/education/presidential-inquiries/establishment-cia. Accessed 15 Aug. 2023.

"National Security Act." Britannica, 31 Aug. 2024, www.britannica.com/topic/National-Security-Act. Accessed 21 Sept. 2024.

Janos, Adam. “Nixon and Johnson Pushed the CIA to Spy on U.S. Citizens, Declassified Documents Show.” History, 11 Jul. 2018, www.history.com/news/cia-surveillance-operation-chaos-60s-protest. Accessed 23 Aug. 2023.

Lind, Dara. “Everyone’s Heard of the Patriot Act. Here’s What It Actually Does.” Vox, 2 Jun. 2015, www.vox.com/2015/6/2/8701499/patriot-act-explain. Accessed 23 Sept. 2024.

“National Security Letters: FAQ.” Electronic Frontier Foundation, www.scribbr.com/citation/generator/folders/2caXniytw4HXPONIKKUMqk/lists/4unGEvkB6xrUc9olioOXso/. Accessed 23 Sept. 2024.

“Surveillance Under the Patriot Act.” American Civil Liberties Union, www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act#:~:text=Hastily%20passed%2045%20days%20after,and%20credit%20reporting%20records%2C%20and. Accessed 23 Sept. 2024.

“Page Rank Algorithm and Implementation.” Geeks For Geeks, 6 Sept. 2022, www.geeksforgeeks.org/page-rank-algorithm-implementation/. Accessed 24 Aug. 2023.

Kopp, Carol M. “What Is a Business Model?” Investopedia, 26 Jul. 2024, www.investopedia.com/terms/b/businessmodel.asp. Accessed 21 Sept. 2024.

Storelli, Alexandre. “Advertising and Mixed Motives (Sergey Brin & Larry Page, 1998).” Alexandre Storelli, 22 Feb. 2022, alexandre.storelli.fr/advertising-and-mixed-motives-sergey-brin-larry-page-1998/. Accessed 21 Sept. 2024.

Bales, Rebecca. “AdSense: Complete Guide — History, Products, Founding, and More.” History Computer, 1 Dec. 2022, history-computer.com/technology/adsense-history/. Accessed 21 Sept. 2024.

“Annual Revenue of Google from 2002 to 2023.” Statista, 22 May 2024, www.statista.com/statistics/266206/googles-annual-global-revenue/. Accessed 21 Sept. 2024.

Wood, Therese. “Visualizing the Evolution of Global Advertising Spend (1980-2020).” Visual Capitalist, 10 Nov. 2020, www.visualcapitalist.com/evolution-global-advertising-spend-1980-2020/. Accessed 21 Sept. 2024.

Esguerra, Richard. “Google CEO Eric Schmidt Dismisses the Importance of Privacy.” Electronic Frontier Foundation, 10 Dec. 2010, www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy. Accessed 10 Aug. 2023.

Johnson, Bobbie. “Privacy No Longer a Social Norm, Says Facebook Founder.” The Guardian, 11 Jan. 2010, www.theguardian.com/technology/2010/jan/11/facebook-privacy. Accessed 10 Aug. 2023.

Calver, Tom, and Joe Miller. “Social Site Terms Tougher than Dickens.” BBC, 6 Jul. 2018, www.bbc.com/news/business-44599968. Accessed 12 Aug. 2024.

Sandle, Tim. “Report Finds Only 1 Percent Reads ‘Terms & Conditions’.” Digital Journal, 29 Jan. 2020, www.digitaljournal.com/business/report-finds-only-1-percent-reads-terms-conditions/article/566127. Accessed 12 Aug. 2024.

Stone, Brad, and Brian Stelter. “Facebook Withdraws Changes in Data Use.” New York Times, 18 Feb. 2019, www.nytimes.com/2009/02/19/technology/internet/19facebook.html. Accessed 12 Aug. 2024.

“Art. 12 GDPR.” Intersoft Consulting, gdpr-info.eu/art-12-gdpr/. Accessed 12 Aug. 2024.

Chapman, Samuel. “Big-Tech Data Collection: What They Know & How to Protect Your Information Online in 2024.” Privacy Journal, 18 Mar. 2024, www.privacyjournal.net/big-tech-data-collection/#what-big-tech-companies-know-about-you. Accessed 12 Aug. 2024.

“How Companies Gather Data & What They Do With It.” Icreatives, 18 May 2021, www.icreatives.com/iblog/how-companies-collect-data/. Accessed 12 Aug. 2024.

Wagner, Nicole. “6 Types of Behavioral Data That Can Be Used For Segmentation.” Stevens Tate, 8 Sept. 2023, stevens-tate.com/articles/behavioral-data-used-for-segmentation/. Accessed 14 Aug. 2024.

Mitchell, Cory. “What Is an IP Address?” Investopedia, 14 Jul. 2024, www.investopedia.com/terms/i/ip-address.asp. Accessed 12 Aug. 2024.

“How To Collect Engagement Data and Improve Customer Engagement in SaaS.” Usepilot, 30 Jun. 2023, userpilot.com/blog/engagement-data/. Accessed 15 Aug. 2024.

Planovsky, Kevin. “Seven Types of Ad Targeting to Help You Hit the Spot.” Croud, 22 Nov. 2023, croud.com/en-us/resources/seven-types-of-ad-targeting-to-help-you-hit-the-spot/. Accessed 16 Aug. 2024.

“Can My Phone Be Tracked If Location Services Are Off?” McAfee, www.mcafee.com/learn/can-my-phone-be-tracked-if-location-services-are-off/. Accessed 18 Aug. 2024.

“What Is GPS?” GPS.GOV, www.gps.gov/systems/gps/. Accessed 18 Aug. 2024.

“Niche.” Merriam Webster., www.merriam-webster.com/dictionary/niche. Accessed 19 Aug. 2024.

Market Research Future, & Vyas, G. (2014, September). Data Broker Market Size, share, industry growth 2032. Market Research Future., https://www.marketresearchfuture.com/reports/data-broker-market-11676#:~:text=Data%20Broker%20Market%20Overview,period%20(2023%20%2D%202032) Accessed 22 Sep, 2024.

Boyle, Alyssa. “What Is A Data Broker?” Ad Exchange, 24 Mar. 2024, www.adexchanger.com/adexplainer/what-is-a-data-broker/. Accessed 24 Aug. 2024.

Duhigg, Charles. “How Companies Learn Your Secrets.” New York Times, 16 Feb. 2012, www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=6&_r=1&hp. Accessed 23 Aug. 2024.

Segal, Troy. “Silicon Valley: Definition, Where It Is, and What It’s Famous for.” Investopedia, 27 Aug. 2024, www.investopedia.com/terms/s/siliconvalley.asp. Accessed 22 Sept. 2024.

Hayes, Adam. “Subcontracting: How It Works, Benefits, Definition, and Taxation.” Investopedia, 29 Apr. 2024, www.investopedia.com/terms/s/subcontracting.asp. Accessed 22 Sept. 2024.

"Digital Destroyers How Big Tech Sells War on Our Communities." Big Tech Sells War, bigtechsellswar.com/. Accessed 22 Sept. 2024.

González, Roberto J. "The Rise of Silicon Valley'S Digital Defence Industry." TNI.ORG, 7 Feb. 2023, www.tni.org/en/article/militarising-big-tech. Accessed 22 Sept. 2024.

Khanal, Shaleen, et al. "Why and How Is the Power of Big Tech Increasing in the Policy Process? The Case of Generative AI." Policy and Society, 2024, pp. 1-18, https://academic.oup.com/policyandsociety/advance-article/doi/10.1093/polsoc/puae012/7636223. Accessed 22 Sept. 2024.

Hartmans, Avery, and Beatrice Nolan. "Meet Sheryl Sandberg: Meta's Former Chief Operating Officer Who Just Announced She's Leaving Meta's Board of Directors." Business Insider, www.businessinsider.com/sheryl-sandberg-former-coo-facebook. Accessed 22 Sept. 2024.

Salmon, Felix. "Who Is Larry Summers, the Controversial Pick to Join OpenAI's Board." Axios, 22 Nov. 2023, www.axios.com/2023/11/22/larry-summers-openai-board. Accessed 22 Sept. 2024.

Fernando, Jason. "Cambridge Analytica: Overview, History, Example." Investopedia, 30 Oct. 2021, www.investopedia.com/terms/c/cambridge-analytica.asp. Accessed 22 Sept. 2024.

Ghoshal, Devjyot. "Mapped: The Breathtaking Global Reach of Cambridge Analytica'S Parent Company." QZ, 28 Mar. 2018, qz.com/1239762/cambridge-analytica-scandal-all-the-countries-where-scl-elections-claims-to-have-worked. Accessed 22 Sept. 2024.

Scott, Mark. “Cambridge Analytica Did Work for Brexit Groups, Says Ex-staffer.” Politico.Com, 30 Jul. 2019, www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook/.*

Watkins, Eli. “Cambridge Analytica Announces Closure.” CNN.Com, 16 May 2018, edition.cnn.com/2018/05/02/politics/cambridge-analytica-closure/index.html. Accessed 22 Sept. 2024.

“National Polls.” Projects.Fivethirtyeight.Com, 8 Nov. 2016, projects.fivethirtyeight.com/2016-election-forecast/national-polls/.

DeSmith, Christy . “Election Forecasts Often Miss. Annoying, Yes, But Real Problem for Scholars.” The Harvard Gazette, 28 Mar. 2023, news.harvard.edu/gazette/story/2023/03/researchers-come-up-with-a-better-way-to-forecast-election-results/. Accessed 22 Sept. 2024.

Stegmaier, Mary, and Helmut Norpoth. “Election Forecasting.” Oxford Bibliographies, 27 Jun. 2017, www.oxfordbibliographies.com/display/document/obo-9780199756223/obo-9780199756223-0023.xml. Accessed 14 Aug. 2024.

“Who Will Win the Presidency?” Projects.Fivethirtyeight.Com, 8 Nov. 2016, projects.fivethirtyeight.com/2016-election-forecast/. Accessed 22 Sept. 2024.

Auchard, Eric, and David Ingram. “Cambridge Analytica CEO Claims Influence on U.S. Election, Facebook Questioned.” Reuters.Com, 21 Mar. 2018, www.reuters.com/article/business/cambridge-analytica-ceo-claims-influence-on-u-s-election-facebook-questioned-idUSKBN1GW1SG/. Accessed 22 Sept. 2024.

Cadwallad, Carole, and Emma Graham-Harrison. “Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach.” The Guardian, 17 Mar. 2018, www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Accessed 22 Sept. 2024.

Boag, Keith. “Money Man.” CBC, www.cbc.ca/news2/interactives/sh/wex94ODaUs/trump-robert-mercer-billionaire/#article. Accessed 22 Sept. 2024.

“Steve Bannon.” Britannica, 31 Aug. 2024, www.britannica.com/biography/Steve-Bannon. Accessed 22 Sept. 2024.

Wong, Julia C., et al. “How Academic at Centre of Facebook Scandal Tried – and Failed – to Spin Personal Data into Gold.” The Guardian, 24 Apr. 2018, www.theguardian.com/news/2018/apr/24/aleksandr-kogan-cambridge-analytica-facebook-data-business-ventures. Accessed 22 Sept. 2024.

“Psychometric Profiling.” METTL, mettl.com/glossary/p/psychometric-profiling/#:~:text=Psychometric%20profiling%20is%20the%20process,%2C%20objective%2C%20and%20structured%20approach. Accessed 22 Sept. 2024.

Cadwalladr, Carole. “‘I Made Steve Bannon’s Psychological Warfare Tool’: Meet the Data War Whistleblower.” The Guardian, 18 Mar. 2018, www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump. Accessed 22 Sept. 2024.

Hern, Alex. “Cambridge Analytica: How Did It Turn Clicks into Votes?” The Guardian, 6 May 2018, www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump. Accessed 22 Sept. 2024.

Ingram, David. “Factbox: Who Is Cambridge Analytica and What Did It Do?” Reuters, 20 Mar. 2018, www.reuters.com/article/technology/factbox-who-is-cambridge-analytica-and-what-did-it-do-idUSKBN1GW07F/. Accessed 22 Sept. 2024.

Hartmans, Avery. “It’s Impossible to Know Exactly What Data Cambridge Analytica Scraped from Facebook — But Here’s the Kind of Information Apps Could Access in 2014.” Business Insider, www.businessinsider.com/what-data-did-cambridge-analytica-have-access-to-from-facebook-2018-3. Accessed 22 Sept. 2024.

Chang, Alvin. “The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram.” Vox, 2 May 2018, www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram. Accessed 22 Sept. 2024.

Williams, Sarah. “What Information from Your Voting Record Is Public?” FindLaw, 26 Mar. 2024, www.findlaw.com/voting/how-u-s--elections-work/what-information-is-public-from-your-voting-record.html. Accessed 18 Sept. 2024.

Darby, Jayson. “What Are the Big 5 Personality Traits?” Thomas.Co, 28 Jun. 2024, www.thomas.co/resources/type/hr-guides/what-are-big-5-personality-traits#:~:text=The%20five%20broad%20personality%20traits,developed%20in%201949%20by%20D.%20W. Accessed 19 Sept. 2024.

Lim, Annabelle G. “Big Five Personality Traits: The 5-Factor Model Of Personality.” Simply Psychology, 20 Dec. 2023, www.simplypsychology.org/big-five-personality.html. Accessed 22 Sept. 2024.

Resnick, Brian. “Cambridge Analytica’s “Psychographic Microtargeting”.” Vox, 26 Mar. 2018, www.vox.com/science-and-health/2018/3/23/17152564/cambridge-analytica-psychographic-microtargeting-what. Accessed 22 Sept. 2024.

Lewis, Paul, and Paul Hilder. “Leaked: Cambridge Analytica’s Blueprint for Trump Victory.” The Guardian, 23 Mar. 2018, www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory. Accessed 22 Sept. 2024.

Mangwana, Nick. “Confronting Name-Dropping Scourge.” Herald.Co.Zw, 20 Jun. 2024, www.herald.co.zw/confronting-name-dropping-scourge/. Accessed 14 Aug. 2024.

Rotondi, Jessica P. “What Are Swing States and Why Are They Critical in US Elections?” History, 7 Oct. 2020, www.history.com/news/swing-states-presidential-elections. Accessed 22 Sept. 2024.

McNeil, Taylor . “Did Cambridge Analytica Sway the Election?” Tufts Now, 17 May 2018, now.tufts.edu/2018/05/17/did-cambridge-analytica-sway-election. Accessed 14 Aug. 2024.

Ray, Michael. “How Does the Electoral College Work?” Britannica, www.britannica.com/story/how-does-the-electoral-college-work. Accessed 14 Aug. 2024.

“Split Electoral Votes in Maine and Nebraska.” 270towin, www.270towin.com/content/split-electoral-votes-maine-and-nebraska/. Accessed 14 Aug. 2024.

“Distribution of Electoral Votes.” 270towin, www.archives.gov/electoral-college/allocation. Accessed 14 Aug. 2024.

“Texas.” 270towin, www.270towin.com/states/Texas. Accessed 14 Aug. 2024.

“California.” 270towin, www.270towin.com/states/California. Accessed 14 Aug. 2024.

Bhardwaj, Prachi, and Samantha Lee. “Here’s a State-by-State Breakdown of Facebook Users Impacted by the Cambridge Analytica Scandal.” Business Insider, www.businessinsider.com/facebook-cambridge-analytica-affected-us-states-graphic-2018-6. Accessed 14 Aug. 2024.

Brownstein, Ronald. “How the Rustbelt Paved Trump’s Road to Victory.” The Atlantic, 10 Nov. 2016, www.theatlantic.com/politics/archive/2016/11/trumps-road-to-victory/507203/. Accessed 14 Aug. 2024.

Wallenfeldt, Jeff. “Rust Belt.” Britannica, 1 Sept. 2024, www.britannica.com/place/Rust-Belt. Accessed 22 Sept. 2024.

“New York.” 270towin, www.270towin.com/states/New_York. Accessed 14 Aug. 2024.

“Pennsylvania.” 270towin, www.270towin.com/states/Pennsylvania. Accessed 14 Aug. 2024.

“Ohio.” 270towin, www.270towin.com/states/Ohio. Accessed 14 Aug. 2024.

“Michigan.” 270towin, www.270towin.com/states/Michigan. Accessed 14 Aug. 2024.

“Wisconsin.” 270towin, www.270towin.com/states/Wisconsin. Accessed 14 Aug. 2024.

“Indiana.” 270towin, www.270towin.com/states/Indiana. Accessed 14 Aug. 2024.

“Iowa.” 270towin, www.270towin.com/states/. Accessed 14 Aug. 2024.

“Illinois.” 270towin, www.270towin.com/states/Illinois. Accessed 14 Aug. 2024.

“Missouri.” 270towin, www.270towin.com/states/Missouri. Accessed 14 Aug. 2024.

“Washington.” 270towin, www.270towin.com/states/Washington. Accessed 14 Aug. 2024.

“Oregon.” 270towin, www.270towin.com/states/Oregon. Accessed 14 Aug. 2024.

"Colorado." 270towin, www.270towin.com/states/Colorado. Accessed 14 Aug. 2024.

"New Mexico." 270towin, www.270towin.com/states/New_Mexico. Accessed 14 Aug. 2024.

"Montana." 270towin, www.270towin.com/states/Montana. Accessed 14 Aug. 2024.

"SouthDakota." 270towin, www.270towin.com/states/South_Dakota. Accessed 14 Aug. 2024.

"2016 Presidential Election Results." Politico, www.politico.com/2016-election/results/map/president/. Accessed 14 Aug. 2024.

Enten, Harry. "How Much Did WikiLeaks Hurt Hillary Clinton?" FiveThirtyEight, 23 Dec. 2016, fivethirtyeight.com/features/wikileaks-hillary-clinton/. Accessed 14 Aug. 2024.

Gerstein, Josh. "Trump Can't Get It Right on Clinton's Email Deletion." FiveThirtyEight, 9 Oct. 2016, www.politico.com/blogs/2016-presidential-debate-fact-check/2016/10/trump-cant-get-it-right-on-clintons-email-deletion-229469. Accessed 14 Aug. 2024.

Videos and Documentaries:

Terms and Conditions May Apply. Directed by Cullen Hoback, Variance Films, 2013.

"How Cambridge Analytica Exploited the Facebook Data of Millions." YouTube, uploaded by The New York Times, 9 Apr. 2018, www.youtube.com/watch?v=mrnXv-g4yKU.

"المعرفة الإمبريالية| عبدالوهاب المسيري." YouTube, uploaded by NAGM, 27 Feb. 2021, www.youtube.com/watch?v=008RByhKMSg