EMERSON COLLEGE

HONORS PROGRAM

Corrupting Pandora:

How the Economic Imperatives of Surveillance Capitalism are Degrading the Internet's Potential

An Honors Thesis

submitted by

Isaiah Anthony

to the Honors Program of Emerson College

in partial fulfillment of the requirements for

the degree of

Bachelors of Science

in

Journalism

Emerson College

Boston, Massachusetts

Spring, 2022

Abstract

Corrupting Pandora:

How the Economic Imperatives of Surveillance Capitalism are Degrading the Internet's Potential

by

Isaiah Anthony

Emerson College

Spring, 2022

Advisor: Meta Wagner

This paper addresses the emerging economic sector of surveillance capitalism, which functions on the harvesting, analysis, and selling of data, obtained through user engagement with online platforms such as Facebook, Google, Amazon, and more. The highly lucrative practice not only violates the privacy of internet users, but has also created an economic framework of data colonialism that has spread rapidly throughout the tech sector,12 recalibrating the goals of the Internet from liberating creation to incessant collection. This paper argues that the immense potential of the Internet as a tool for the common good is being threatened by the allure of guaranteed profits offered by the adoption of surveillance capitalism.

Table of Contents

Introduction: Here Comes Trouble

As a member of a generational class dubbed the "digital natives," I have grown up alongside the digital softwares that now exist as cornerstones of modern communication. Having spent my most developmental years actively engaging in online spaces, the internal rules and mechanism of these spaces are known to me as well as scripture to my parents. Generation Z can accurately be coined the 'troubleshooters' for their acute ability to understand how to operate a user interface without instruction, solely on intuition and knowledge of common operating procedures.

Before I had access to the internet, I already understood how important it was that I get in on the action. All the school cafeteria jokes came from Youtube videos. All the funny kids tweeted. The internet was where things were happening, where culture emerged.

So when I finally got connected, I never looked back. Youtube, Facebook, Twitter, Instagram, Snapchat, and more platforms that didn't stand the test of time, were all my places of escape. I never needed to be bored. I never needed to be alone. These services were in the palm of my hand, ready to give me whatever I wanted.

And by God, I took it. Soon I had mastered the rules of the digital environment. I knew how to fix a buffering Youtube video before I knew the branches of government. I knew how to stalk someone digitally before I learned to drive.

It is only now, after any potential damage has already been done, that I ask myself: was that okay? Was I safe? There was always talk of the dangers of other *users* - pedophiles, creeps, kidnappers, lurking in wait for children online - but I do not recall much discussion on potential threats coming from the operators of the online space. Now, I surely have a digital footprint the

size of an eighteen wheeler, mostly on account of decisions I made before I was old enough to vote. I'm tech savvy - I can fix my grandmother's computer without breaking a sweat - but what did I lose: my identity, my anonymity, my autonomy? What was taken from me, and how might future generations, who are at this very moment circumventing any and all age-barriers haphazardly implemented to keep underage users out, be better protected from digital companies looking to turn them into data streams?

Before any spirits get raised, none of these questions will be properly answered in this paper. The easy decision, to hit the ultimate off-switch and kill the Internet before it does further damage, is not one I support. Whether I like it or not, the Internet is a part of me, and I see the good in it. I believe I'm a more compassionate, well-informed, intelligent individual because of the hyper-connectivity afforded to me by the Internet. But as the digital age churns along, as money and power continues to flow in the direction of anyone who can get data-rich users to their website, we must address the rising dilemmas threatening to corrupt online spaces beyond repair.

This paper serves to highlight where development is headed in the wrong direction, how these bad-faith drives came about, and what may be lost should the current course of technological advancement continue.

Part 1: A Future Yet Unrealized

In the few decades since its conception, the internet has redefined and recalibrated human life, offering an unprecedented infrastructure of connectivity and collaboration across the globe. Distance no longer hinders communication. Physicality is no longer a condition of commerce.

Information no longer knows scarcity. Computing no longer operates at the individual hardware level but instead melds seamlessly with a network of connected devices to create a global canvas of technological might.

The internet is the single most powerful informational tool ever created by humanity. In its mechanisms lies the potential to tackle every plague and dilemma that humanity faces, now and in the future. With the abilities made possible by the internet; large-scale computing, global collaboration, and mass data analysis; there has never been a time in human history where unity, equality, and harmony were more in reach.

Should the development of the internet continue on its present course, all of this potential will be squandered, killed in the interests of corporate profit.

While the power of the internet is continually being explored, expanded, and realized, the motivations and logics of the companies at the helm of this growth are operating in the interests of shareholders, not the betterment of humanity. As more companies emerge seeking to plant roots in the digital sphere, they are increasingly aligning themselves with a new form of capitalism, unique to the internet, that actively deteriorates both online and offline spaces.

Surveillance capitalism, a term coined by Shoshana Zuboff in her 2019 book, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, is an economic model centered around the extraction and accumulation of massive caches of data generated by internet-enabled devices. Using data points ranging from geographical location, web habits, purchasing history, and much more, Big Tech companies, including but not limited to Google, Facebook, Apple, and Amazon, use their colossal engines of computing to analyze and interpret user behavior with the goal of hyper-accurate prediction algorithms and, ultimately,

behavioral modification. The public-facing side of these companies, selling internet-enabled devices and offering free online services, is the bait used to add more data-generating users to their surveillance network. As Zuboff writes, "Surveillance capitalism's products and services are not the objects of a value exchange. They do not establish constructive producer-consumer reciprocities. Instead, they are the 'hooks' that lure users into their extractive operations in which our personal experiences are scraped and packaged as the means to others' end" (Zuboff 10).

This has proved to be an incredibly profitable business model, with companies from all economic sectors pursuing the dream of behavioral certainty among their consumers. The logics of surveillance capitalism has propelled the tech sector into an economic boom, flooding Silicon Valley with massive capital investments with the promise of guaranteed profits.

All of this comes at the expense of the user, whose habits, behaviors, and individuality are stripped away, harvested, and sold to the highest bidder. The impact of this business model is difficult to comprehend because there has never been an intrusion of such scale.

The unprecedented nature of surveillance capitalism benefits its operators. At present, there is little to no legislation or regulation prohibiting the practices that prop up the surveillance economy, and Tech leaders are capitalizing on government ineptitude, establishing their business practices as commonplace, hiding their true operations behind a shiny veneer. The hope is that once regulators catch on to the gambit, the engine of surveillance capitalism will be too crucial for too many economic sectors to be dismantled.

The motivation behind data harvesting, in the eyes of the general public, is largely misconstrued. Gone are the days when user trends and habits were recorded merely to increase website engagement. Now, tech companies offer up their data caches for sale, generating

immense profits while doing so. According to an article from *The Reboot*, data brokers, companies who buy and sell data from harvesting sites such as Facebook,

> generate profits by compiling a profile of you from your data trail and then selling it to the highest bidder — banks, insurers, prospective employers, and many others. They can sell individual data profiles as well as lists of people. Some of the categories these companies use to identify and classify individuals include rape victims, erectile dysfunction sufferers, alcoholics, and people who have AIDS or HIV. It was recently revealed that Facebook allows advertisers to target children as young as 13 who have been profiled as being interested in smoking, alcohol, online dating, extreme weight loss, and gambling. (Véliz 2021)

Not only are the extraction practices of surveillance capitalism intrusive and abhorrent, but the products of this operation, behavioral prediction algorithms, are harmful to those subjected to them. By predicting what users want to see and want not to see, tech platforms such as Google and Facebook are seizing control of information access. Deciding what is 'relevant' for users to see strips away the information autonomy that lay at the core of the grand potential of the internet. Instead, users are left with echo-chamber platforms that feed them what the algorithm has determined will keep them engaged. Whether that is an accurate depiction of reality is unimportant.

In a study published in the *Journal of Broadcasting & Electronic Media* titled "Do Search Engines Endanger Democracy? An Experimental Investigation of Algorithm Effects on Political Polarization," the researchers determined there to be a link between predictive algorithms and increased political polarization, stating

> Thus, algorithmic recommendations personalized by user behavior data, if unchecked, has the potential to solidify personal political convictions and encourage polarized opinions. If our findings from YouTube can be generalized to search engines and algorithms running on other online platforms, algorithms and big data are responsible, at least in part, for the increasingly divisive political culture in many contemporary democracies. (Cho 16)

In hiding dissenting stances, digital platforms are herding users into isolated spheres of influence, lowering critical thinking and increasing the spread of misinformation.

State of the Literature

As digital platforms have become an increasingly prominent aspect of the function of United States workflow, social life, and infrastructure, many writers, scholars, and researchers have begun analyzing the functionality of the software infrastructure of these highly influential platforms. In the case of two major digital platforms, Google and Facebook, a number of books and papers have been published in recent years detailing the flaws present in their designs. Looking specifically at algorithmic-based content personalization, a subsection of academic research has been conducted demonstrating the dangers of these systems.

Media studies scholars encounter a number of challenges when studying digital platforms, whose owners go to great lengths to maintain utmost secrecy surrounding the algorithms that dictate content displayed. Crude empirical studies have been conducted that offer glimpses into the inner working of these systems, revealing biases (Al-Abbasa) and polarization effects (Cho), but analytical deep dives into the infrastructure of digital platforms are difficult

since such platforms have no obligation, nor incentive, to provide access to researchers. Additionally, Tech companies have recently gone on the attack against those investigating the inner workings of these digital platforms, with Facebook going so far as to deplatform a group of researchers who published a study revealing the rampant spread of misinformation on the platform (Muruf 2021).

Despite this, there is a growing body of research.

Before continuing, readers are encouraged to perform an exercise carefully designed to place them in the proper frame of mind to understand the originating point of the arguments made in this paper.

Exercise 1

Required materials: an Amazon Alexa Dot, a wooden baseball bat.

Instructions: place the Amazon Alexa-enabled device on a sturdy surface clear of any fragile items or individuals. In rapid succession, vigorously connect the end of the baseball bat with the plastic casing of the Alexa-enabled device. Do this until the exterior of the device is fractured beyond repair and the entrails of the machine are visible with the naked eye. Observe the physicality of the piece of broken technology. Observe your role in having destroyed it. For further comprehension, plug the machine into an outlet and attempt to have it tell you the week's weather forecast. If bashed as instructed, it will be unable to understand your question. This is because of the baseball bat that turned its motherboard to shrapnel, its plastic casing to a mangled mess, its smiling Amazon logo to an unrecognizable blot. All of this came about

because you, the wielder of the baseball bat, exercised your strength and prowess over the machine constructed with the cheapest parts available.

This exercise serves not only to render as many Amazon sensors inoperable as possible but also to demonstrate the fragility of surveillance capitalism and its purveyors. There is nothing special, divine, immortal, or transcendent about these devices. They are simply cogs of a larger engine, tendrils of a greedy beast that feeds on information. When separated from their host, they are quite easy to turn to mince-machines. Surveillance capitalism can be dismantled.

Imagine a meteor, hurtling through the cosmos at breakneck speed. It has no charted course, apart from its unwavering momentum. It is simply moving forward in the direction from which it came. In the vastness of space, it could be ages before it flies near a body of mass powerful enough to pull it into its orbit. Until then, it will continue on its way, undisturbed, because that is where its momentum is taking it, and its momentum is remarkably strong.

If someone, something, found itself in the path of the meteor and foresaw the consequences of a direct collision, how would they best divert the chunk of space rock hurdling their way? Would they try and stop it in its tracks? Maybe, but this would require them to muster up a counter-force equal to or greater than the velocity of the meteor in order to slow it down to a halt. The problems continue to mount when the meteor reaches their sphere of orbit and begins redirecting and speeding up in their direction.

What can these sorry souls do to avoid this calamity? They don't have the numbers or the strength to stop the meteor or turn it around. But what strength they do have can alter the course of the meteor slightly. Perhaps they can nudge, poke, and jab at the side of the approaching

meteor until its course is adjusted to land in an uninhabited region or a body of water, minimizing the damage. Perhaps they can salvage the space rock after the crash, using the minerals found within to make novelty space-ore keychains commemorating their victory over the forces of nature and space.

The meteor currently threatening humanity is the economic imperatives dictated by surveillance capitalism.

This paper by no means seeks to reverse the course of technological advancement, only to alter its direction towards a direction more suitable for all humanity, not just the select few who own and control the technological means. The benefits, both literal and potential, of mass data analytics and ubiquitous computing are limitless, but so too are the dangers and room for pitfall and malice. The struggle of the moment is that these malicious incarnations of technology are solidifying themselves in the public eye as the set course for technology. This puts modern humanity on a course with two paths: the technophiles bring about their dream of a predictive state where their sensors can guarantee positive market outcomes for those in on the con, apathetic towards the interests of the gutter rats generating their highly lucrative data points; alternatively, humanity could reject the economic imperatives of Silicon Valley firms and harness the immense power of technology as a force for social good. The almighty engines of the internet could be rerouted to tackle the problems of the people, not the board members.

The primary chain link currently shackling modern society to the market-based interests of Big Tech is its own imagination for what technology is capable of achieving. The CEOs and marketing departments of tech firms incessantly preach their twisted gospel of technological determinism, but their aim is more so to pigeonhole humanity's understanding of technology's

power within the context of their economic aims. What might the young, technologically savvy minds of the world be able to achieve, were they not corralled into Palo Alto cubicles serving the interests of a class of corporate elite? What societal blights might be eradicated with the collective brainpower and technological capabilities of this empowered generation, were they only given the tools to do so? Until humanity reconciles with and frees itself from the generational baggage of its ugly past - colonialism, neoliberalism, imperialism, capitalism - it will continue to grow with these interests deep in its roots, corrupting the buds and branches bursting forth as new fields of technology and innovation emerge. Technology is innocent; People are guilty. With the right adjustments, nudges, and course corrections, the present era of technological development can be harnessed for the betterment of humanity.

If the material technology is innocent, what corrupts it? Humans? That would not be an unfair answer, but blaming the creation of the monster solely on the malice of the creator minimizes the logics and circumstances that motivated the creation and subsequent corruption. The present state of technological development, which finds its ideological heartland in Silicon Valley, has allowed itself to be overtaken by the ever-greedy economic imperatives that come to dominate and oppress all facets of innovation under a regime of unfettered capitalism. The free market, ironically, has coerced and cajoled the key figures of the tech sector into limiting the potential of their innovations to serve only the interests of the market.

Surveillance capitalism is another entry in a long line of exploitation-based business models that have corrupted human innovation. Zuboff writes that "surveillance capitalism is not technology; it is a logic that imbues technology and commands it into action" (Zuboff 15). The internet, data analytics, and personal computing can all exist without the model of surveillance

capitalism. Surveillance capitalism, however, cannot exist without these things. It is this ideology, this market logic, that must be done away with. The only ones who serve to lose from this alternative vision are ultra-wealthy investors not worthy of pity.

There is so much good that could be done with the increasing power of data-analytical technology, yet all the board members, shareholders, and corporate overlords of the sector have inflicted upon themselves a case of tunnel vision that can only come about by capitalism run amok. In seeing the power of technology as monolithic, with the highest potential being maximum financial profit, the culture of technological innovation in the United States is handicapped.

Through prediction and behavioral certainty algorithms, big tech firms are impeding the free will of their multitude of users. This dream of guaranteed response and interaction is veering the technological sector into a new economic model dependent on the exploitation of users. The present trajectory of technological progress is a result of unfettered capitalism, Silicon Valley delirium, advertising anarchy, and greed. Without reform, regulation, and logic recalibration, humanity may squander the potential of the most powerful tool of the time, large-scale computing, data analytics, and digital omnipresence. Make no mistake, the war machine of Big Tech, made up of the most technologically advanced minds in history, has the power to eliminate many of the hindrances that have plagued humanity since the beginning. To do so, however, it must be free from the narrow-minded focus of capitalism, free from the yolk of shareholders apathetic to anything but profit. The future lies waiting in Silicon Valley, waiting to be liberated from its current occupation. It is being crippled, shoehorned into a field undeserving of its power.

Were the power of technology to be realized beyond its potential to make money, humanity's future would dramatically change course for the better.

Resistance to an emerging economic sector is not resistance to capitalism itself, as the free market evangelists might claim, but a crucial element in the upholding of a rational capitalist framework, where the interests of the corporation are tethered to the land and its people. Surveillance capitalism is a mutation of the market, allowed to thrive on account of its profit potential. There exists a future where the mechanisms of the surveillance capitalist machine are reworked for the good of all people. In order for this to come to fruition, however, the market must be tethered to the will and needs of the people.

Approaching the problems presented here strictly with the precedence of the past only hinders potential and enables the continued market transformation into a surveillance model. It's not enough to throw 'monopoly' labels at big tech firms, such as Google and Facebook, and demand them to be broken up. All this would accomplish is a hole in the market waiting to be filled by the next surveillance capitalist firm. New logics must be established and enshrined with these capitalistic mutations in mind in order for the sector to develop with interests aligned with the population.

Silicon Valley tech evangelists preach that technology moves the world forward. There is truth to this, but not much they would agree with. A more accurate wording would be this -- the market spawns economic imperatives that the Silicon Valley capitalists adopt as gospel, developing technology not around society, but around the dominant imperative. As the imperative grows it forms a market of its own, pushing more of the tech into the world and constructing a culture around the 'innovation.' Once the technology is adapted into a proper

economy of scale, it has reached enough people to influence society. However, that influence is not from the so-called sacred potential of the hardware/software of the product, but instead a byproduct of a society subservient to the economic imperatives of the elite class.

Part 2: Paving the way for the Present Order

Surveillance capitalism is a product of its time. The mechanisms of this economic sector could only thrive in the present era for more reasons than simply technological advancement. Looking into the near past, a number of incidents, events, and decisions paved the way for the unchecked growth of the unknown business model, the deterioration of personal privacy, and the present corporate surveillance state.

The companies driving the expansion of the surveillance economy have succeeded in avoiding government regulation by capitalizing on the digital naivety of the present governing order as well as utilizing the state's present surveillance-heavy framework.

Fear and Subjugation: The War on Terror and the Surveillance Machine

The Internet emerged on the scene at a unique moment in history, when rules were being rewritten, definitions were being changed, and lines were being muddled. Newly conceived technologies, industries, and economies are developed to fill a hole in the system in which they operate, and the Internet is no different. When the world changed direction following the terror attacks on 9/11, so too did the Internet. It became evident that this tool, designed for open, limitless, seamless communication, could be co-opted into a tool of state control and

surveillance, which the United States government, devastated, scared, and embarrassed following an attack on their soil, sought desperately.

In the wake of the attacks on the World Trade Center and the Pentagon, the United States Government sought by any means necessary to prevent another attack on U.S. soil. This response came at the expense of the privacy and liberty of residents of the United States.

Six weeks after the attacks, as the nation mourned the lost and fearfully awaited the much talked about next attack, congress passed the USA/Patriot Act. This legislation expanded the authority of law enforcement agencies to conduct domestic mass surveillance in search of potential terror threats, as well as removing power checks and gutting operational oversights. The Patriot Act expanded existing exemptions in the Bill of Rights to legitimize a systemic surveillance state.

The Patriot Act was passed in the fog of tragedy, seen as a remedy for the fear crippling the country. It was a draconian bargain. By forfeiting rights to privacy, United States citizens may be able to sleep at night. Congress members were pressured to pass the bill, their judgments impaired by fear, revenge, and an overwhelming desire to not be blamed for the hypothetical next attack.

But this bargain had another layer to it, one that tainted the already murky nature of the violating practices being legalized. The contents of the Patriot Act were not drawn up in the wake of the attacks. They were not meticulously written with Al-Qaeda in mind. A large number of the contents of the Patriot Act were existing desires of United States law enforcement agencies, looking to expand their reach and authority. Many of the tools already existed for foreign

intelligence gathering. The Patriot Act simply allowed for the surveillance apparatus to be turned inward onto the residents of the United States.

This is most evident in the case of the National Security Agency, which operates as the intelligence branch of the government. Three days after the towers fell, the NSA began monitoring the digital communications of residents of the United States who were in contact with any individuals residing in countries deemed to be terror hotspots. This was done without permission, without warrants, and without disclosure or announcement. While their operations were later given approval by the Bush administration, the speed at which the NSA began these operations is telling. There was no time needed to establish the framework or technological infrastructure to conduct this domestic surveillance. That is because the tools were already in place, and the agency simply needed a tragedy to warrant its push to expand its operations (Pilkington 2021).

The 9/11 attacks were an opportunity to get these violating, unconstitutional measures enshrined into law. While the narrative around the passing of the Patriot Act was that it was a temporary measure to combat the current terror dilemma, that was never the case. That is why, twenty years after the bills passing, with the War on Terror existing now as little more than a narrative, it is still in place (“Surveillance under the USA/Patriot Act").

The passing of the Patriot Act normalized the invasion of privacy by citing national security. In doing this, the notion of privacy decayed, repainted as something inherently suspicious. Reflecting on Marxist theory in the era of Big Tech, Christian Fuchs writes that "surveillance ideology has helped create a culture of control, fearmongering, scapegoating, suspicion, competition and individualisation" (Fuchs 57). The narrative became 'if you have

nothing to hide, you have nothing to fear.' The naming of the bill was a heavy-handed nod towards the new order. To oppose subjecting oneself to constant surveillance was unpatriotic, akin to supporting terror and betraying the memory of those lost in the ashes of ground zero.

The United States government found opportunity in tragedy, and in doing so they paved the way for the present surveillance economy's unopposed growth.

The Snowden Leak

In 2013, a CIA contract employee named Edward Snowden blew the whistle on the egregious overreach and unchecked power of the National Security Agency. His revelations shed light on the NSA's tools for surveillance and exposed the agency's efforts to mislead both the public and Congress regarding its actions.

Snowden's leaks show the outcome of the Patriot Act a little over a decade after its passing. It revealed the PRISM program (Planning Tool for Resource Integration, Synchronization, and Management), which allowed the NSA to covertly access the data treasure troves of major tech companies (“The Fallout of Edward Snowden and His Leaked Documents, Eight Years Later”). The PRISM program allowed for the NSA to sidestep the courts during their surveillance operations, no longer requiring them to seek warrants and provide probable cause for monitoring of U.S. residents. The program began in 2007, with Microsoft being the first major firm the NSA gained access to. When Snowden leaked documents revealing the program's existence six years later, the list had grown to include Yahoo, Google, Facebook, YouTube, Skype, Apple, and more (Greenwald 2013).

The PRISM program reveals why the United States Government allowed these data empires to grow unhindered. It was beneficial. By collecting vast amounts of data on users, the tech companies were serving the interests of the government. It's a quid pro quo. As long as the government is in on the con, the con will not be stopped.

This alignment of interests illustrates why organized resistance to surveillance capitalism is so difficult. "In the surveillance-industrial complex," Fuchs writes,

> users make data public or semi-public on the Internet. Corporations commodify this data and users' activities to accumulate capital. Secret services and the police aim to gain access to the Big Data flows in order to securitise data and society. In doing so, they partly outsource surveillance to private security services, for whom surveillance is a profitable business. The NSA subcontracts surveillance to more than 2,000 private security companies. In the surveillance-industrial complex, surveillance capital and the surveillance state are fused together. Big Data means Big Brother power and big capitalist business. (Fuchs 58)

Just as the military-industrial complex creates a financial incentive for war, the surveillance-industrial complex creates a financial incentive for invasiveness. With so much money moving back and forth between agencies and corporations, the people have little recourse to resist this new form of subjugation.

In an essay for *Social Research Quarterly*, Jacob Silverman comments on the shifting dynamics of privacy and liberty in the post 9/11 years and the growth of the surveillance system, writing,

> individuals have been made vastly more transparent, while authorities and corporations have become more opaque. These changes in privacy and surveillance track with growth in the US surveillance state.… At the same time, individual rights—while lionized in the public discourse of liberty, freedom, and American exceptionalism—have become frighteningly contingent. Rights for voting, free speech, habeas corpus, to consent to searches, and much more are prone to sudden abrogation under laws that reflect a generalized state of emergency. The enforcement of these measures, in turn, is enabled by the institutionalization of mass surveillance, which allows authorities to monitor social media, record phone calls, film public spaces, track vehicle movements, and strictly control passage at borders with biometric identification. (Silverman 149)

The Patriot Act, the Snowden leak, the PRISM program, and more all reveal how state actions altered the fabric of not only the Internet but the constitution. The fourth amendment of the Bill of Rights ensure "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" (“Constitution of the United States,” am. 4). That amendment is effectively null and void in the digital age. At a time when interpretations of the first and second amendments are routinely crusaded for and championed across a culturally split nation, the fourth amendment has been completely infringed upon. If it can happen to one, it can happen to the others.

The Holy Market: Neoliberalism's role in Surveillance Capitalism

Apart from fear-mongering and tragedy, another political mindset also helped spawn the tech titans currently expanding the surveillance state. The economic framework of neoliberalism that has dominated legislative policy for the past four decades has compromised the integrity of the capitalist system.

In his book, *For Business Ethics: A Critical Approach*, University of Auckland professor Cambell Jones summarizes the rise of neoliberal capitalism, which emerged in the 1970s in response to fears of economic stagflation, stating

> Neoliberalism represents a set of ideas that caught on from the mid to late 1970s, and are famously associated with the economic policies introduced by Margaret Thatcher in the United Kingdom and Ronald Reagan in the United States following their elections in 1979 and 1981. The 'neo' part of neoliberalism indicates that there is something new about it, suggesting that it is an updated version of older ideas about 'liberal economics' which has long argued that markets should be free from intervention by the state. In its simplest version, it reads: markets good, government bad. (Jones 2005)

With neoliberal doctrine at the helm, the market is left to grow in any direction that proves profitable, unhindered, and untethered. Economic interests are not tied to the interests of the people operating in the economic system, but solely to the ability of the elite class to commodify, exploit, and capitalize any available avenue. This has resulted in an economy disconnected from the people. Stock prices rise, profits soar, without raising the standard of

living for the general population. The ideal role of government regulation in matters of economics is to protect the interests of the people, the laborers, to balance out the power of corporations. For close to half a century now, this has not been the case.

As a result, corporations like Google, Facebook, Amazon, and Apple have no incentive or pressure to act in a manner suitable for the population. Under neoliberalism, the only drive is profit, the market is God, and working towards anything without a clear and present monetary incentive is sacrilegious.

In no sector has this created more of a contradiction than the web. The internet has opened the door for a commons of information, communication, and diversity unlike anything seen in history. However, commons are not monetarily profitable. The web, by nature, is post-scarcity. Information can be viewed by anyone with a connection. Files and web pages can be viewed and copied endlessly, without decay. This does not make for high margins.

Fighting back against this grand potential for a connected human species, the profits of neoliberalism at these tech companies have discovered new resources to commodify. This drive has given way to the commodification of data. As Christian Fuchs writes,

> neoliberal capitalism has resulted in the commodification of almost everything, including communication. In the world of digital commodities, we find the commodification of digital labour-power, digital content, digital technologies and online audience. Information is non-rivalrous in consumption (as a resource, information is not used up when consumed). It is difficult to exclude others from access. Information can be easily copied. It is therefore an antagonistic commodity type that can be turned into a commodity, but that can also relatively

> resist commodification and be turned into a common good. Digital capitalism faces a contradiction between digital capital and the digital commons. (Fuchs 54)

The Internet was conceived as an egalitarian tool for communication and information. On its current course, it is morphing into a hierarchical surveillance tool serving its owner, a class of corporate elite, and state agencies. These two futures cannot coexist. Either the free internet will die or the surveillance internet will be stopped.

Before diving into the various tech companies that have sold whatever souls they had to the surveillance cabal, readers are encouraged to partake in the following exercise, carefully crafted to align themselves with the thinking necessary to operate as a surveillance capitalist.

Exercise 2

Required materials: a pen and paper, self-awareness, a friend.

Instructions: Over the course of a day, record your actions in as meticulous detail as possible. Instruct your friend to do so as well. Log where you go, noting when you arrive and when you leave. List everyone you speak to, noting the topics discussed in the conversations. Record every purchase you make, every event and meeting you attend. Note your moods, your attitude, your feelings.

The important part is that you record as much as possible. Everything that can be translated into data should be recorded. Relevance of information should not be considered until after all collection is finished.

At the end of the day, trade logs with your friend. Examine each others' records and attempt to draw inferences about the other's day. Read between the lines. How much can you learn about your friend just through the data?

If done correctly, this exercise should be arduous, annoying, and time-consuming. Consider, then, how this process correlates with your regular life. Each day, you conduct this same data collection process, only its operations are disguised from you. The data is not given to your trusted friend, but to a company that stands to gain from the information you have provided, as well as your government should they seek it out. This is the labor conducted by internet users to serve the surveillance economy.

Reflect on everything you learned about your friend through their data record. How much information did you gain from a single person? What if this same process was conducted on thousands, millions, billions of people? This is the level of information that Big Tech companies are dealing with. You, the user, are their laborer, paid in services designed to trap you in a cycle of engagement rather than fruitful information.

Part 3: The Prophets of the Data Market

Surveillance capitalism and the data economy are invading and influencing all manner of economic markets, far beyond Big Tech. However, without the development of the means of mass surveillance and data extraction developed by major Technology corporations, the system would not have gained the steam seen today. For this reason, it is prudent to explore the major players in Big Tech to analyze each one's contributions and advancements of the mechanisms of the surveillance capitalist framework.

Google

Google was founded in 1998 with the mission to open up the web and create a frictionless information ecosystem. In *The Age of Surveillance Capitalism*, Zuboff writes that "from the start, the company embodied the promise of information capitalism as a liberating and democratic social force that galvanized and delighted second-modernity populations around the world" (Zuboff 67). Led by two Stanford graduates, Google sought to realize the potential of the internet as a means of information egalitarianism.

Google's work with algorithmic precision and data analytics laid the groundwork for the present surveillance data economy. Around the turn of the millennium, Google was a modest digital company that served as a web aggregate. It was not a behemoth of the tech world, a load-bearing pillar of the online world, or a profit-churning business. It recorded $70 million in advertising revenue in 2001 (Johnson 2021), and it remained in the financial limbo of start-up tech ventures.

It was, however, popular. The site executed an estimated 32.8 million searches per day in 2000 (Reid 2021). While this did not translate directly into dollars, the traffic did generate for Google a sizable amount of data, collected from users' search queries.

The initial purpose of data collection at the company was to enhance the performance of the search function, increasing the accuracy of search responses. When Google created new services, the data would be used to help enhance those as well. While this improved the quality of search and the performance of the platform, it was not the profits demanded from investors.

As was the case with many tech startups at the turn of the millennium, Google's popularity was not translating into cash. The company was reluctant to run advertisements that could compromise the integrity of search results, damaging their founding mission and positive reputation. But when the dot com bubble burst in 2000, sending many investment firms and tech startups into a tailspin, Google's founders elected to alter their business model in order to ensure the company's survival (Zuboff 73).

The turning point came when Google realized what they had at their disposal. At the time, of all the data collected, only that which was relevant to search optimization was being utilized, with all other digital trials disregarded. In 2003, Google began harvesting data with a much wider threshold, seizing up all it could from its users. Google had discovered the power of its technology, and it saw a potential for profit from data. Shortly after this, the company went public on the stock market and never looked back (Horvath 2021).

By feeding the accumulated user data into the advanced analytics technology at the company, Google created a way to not only enhance the accuracy of their search results but also enhance the accuracy of the advertisements displayed alongside the results. By gathering up every bit of information it could on users, and drawing conclusions and inferences based around that data, Google could display advertisements to the users most likely to engage with them (Zuboff 78).

This move changed the game. Before this, online advertisement was a lousy fisherman; casting a wide net in the open ocean, relying on repetition and prayer. Click-through rates on online advertisements were abysmal. Google found a way to target advertisements to display only where they would be seen by users with a preexisting, demonstrated interest in the product.

With this higher return rate, Google was able to charge more for ad space on the site, luring in deep pockets with promises of higher click-through rates. Google had found their cash cow in their own servers. With this move, the company planted the seed for the surveillance economy, which would grow into the behemoth of capital seen today.

But the gears of capitalism are not designed to slow down. Google had created a new economic imperative around information accumulation. The subsequent years would see the company growing in new directions, constructing new vacuums through which they could suck in every data bit the world had to offer. Google Maps, launched in 2005, took the surveillance machine to the streets, allowing the company to send their camera-equipped cars down the streets of the world, relaying the findings not only to the public-facing navigation service but also to the company's data coffers.

Google continued its operations, expanding and developing in new directions with the aim of constructing new data streams to enhance its prediction apparatus. The key to Google's success in securing new data collection avenues is speed. The goal is to develop, deploy, and collect before regulatory force or societal backlash can grasp what Google is doing. Zuboff explains that "the company has learned to launch incursions and proceed until resistance is encountered. It then seduces, ignores, overwhelms, or simply exhausts its adversaries" (Zuboff 138). The vagueness of its operations is pivotal to its success; a clear indication of the company's awareness of the questionable ethics and legality of its operations.

The implementation of predictive analytics marked a turning point in Google's journey. Whether they admit it or not, the company's mission changed. It was no longer solely a tool to connect people to the internet, an aggregate of information meant to bring about a revolution of

knowledge and democracy. It was now a tool to connect advertisers to users. This is the result of ascribing to the economic imperatives of tunnel vision capitalism. There is little room for humanity. The only social good allowed is that which can be translated into profit. Google maintains its image in order to remain in good standing with those who truly conduct the labor necessary for its operation, users. By imputing search queries, wearing devices equipped with cameras, sensors and microphones, and more, users conduct free labor that generates the highly lucrative data that keeps Google afloat. "It is crucial to understand that Google lives or dies based on the data it can access and that its strategies are engineered to preserve the openness of the original Web. In a world of closed, siloed information, the search engine would be just a mere tool, not the dominant paradigm it is today" (Wu 281). Google, as is the case with all the free-to-use tech services, operates through the exploitation of its user base.

Through all of this, Google got rich. They faced pushback for their efforts, but never any force strong enough to halt the accumulation machine. As their profits grew and their stocks elevated, the logics of data harvesting spread across Silicon Valley. Emerging companies, unable to construct a profit model for their business, looked to Google's example of transforming the efforts of their users into profits for the company.

One company, an emerging social networking service, jumped head-first into the surveillance economy, changing the course of history, politics, communication, and more.

Facebook

Facebook, launched in 2004, began with the goal of bringing people together. Its mission was to create a social commons for people to connect. It started as a service for college students

at elite universities to digitally lament their intellectual superiority but expanded in 2006 to the general public. On Facebook, people connected with everyone; old roommates, former coworkers, neighbors, friends of friends, friends of friends of friends. People came together.

It was a phenomenon. In his 2018 book, *anti-social media*, Siva Vaidhyanathan encapsulates the cultural discourse surrounding the social media service during its initial boom, stating that "to be without Facebook by 2010 was to miss out on what seemed to be essential conversations and events" (Vaidhyanathan 56). Facebook removed barriers to communication. Friendships, connections, and relationships were no longer limited by geography. People all over the world could talk, argue, virtually farm, share, and engage with each other. And it was all free (until it wasn't). Looking back, it is fascinating to compare the Facebook of old to the malignant, harmful force it is today.

Being free to use was a major selling point for Facebook in the early days. When a user would first visit the site, they would be greeted with the tagline "It's free and always will be." It remains true that users are not charged monetarily for using the service, but Facebook does charge its users in another capacity.

Following the example set by Google, Facebook constructed a data-harvesting, surveillance apparatus to increase revenue. As with Google, this move marks a departure from the original mission of the website. It was no longer a commons of communication where people gathered and connected. Facebook sacrificed its mission at the altar of surveillance capitalism, turning its user base into a data source to be sold at will.

Fuchs writes about how "Facebook's wage share (i.e. the share of the wages it paid from its revenues) was 11%. Why are the company's wages so low in comparison to the total US

economy, and its profits so high? The social media economy is based on the exploitation of users' unpaid digital labour" (Fuchs 60). Facebook users pay for the service with information. They subject themselves to the prying eyes of the algorithms, modeling to keep them engaged as long as possible.

Since Facebook's revenue is reliant on users' continuous digital labor and engagement with the platform, the site is oriented to yield quantity of service instead of quality of service. The all-consuming economic imperatives of surveillance capitalism demand that the site operates not in the interests of crafting productive, positive, healthy connections, but instead in the interests of locking the user into an incessant cycle of engagement and reaction.

The negative impacts of this engagement-based model can not be understated. In their ongoing mission to maximize user engagement, Facebook has cultivated a toxic, malicious environment. It is a breeding ground for misinformation, extremism, and hate.

Engagement does not have to be positive to be profitable. The reason Facebook has dragged its feet in clamping down on misinformation and hate speech is that these things prove so lucrative for the company. For Facebook, it doesn't matter what its users are doing, saying, posting, sharing, planning, scheming, or plotting, as long as they are doing it on Facebook.

Not only is Facebook not incentivized to prevent hate speech and misinformation, but its governing economic imperatives encourage such behavior. Fear, anger, and hate are powerful emotions, and those emotions lead users to engage more with the platform; picking fights, spreading stories, supporting causes. All of this is digital labor generating lucrative data for Facebook. Vaidhyanathan writes that "the reason Facebook does what it does so well--including amplifying the malicious and cruel acts that so many wish to perpetuate on others--is that it

leverages massive amounts of information about its users to effectively sort and send the contents it thinks we want to our feeds. What makes Facebook good also makes it bad. What makes Facebook wealthy also lets us be crueler" (Vaidhyanathan 54). Emotion drives engagement, which produces data. Facebook's financial business model demands that anything that results in more data without resulting in detrimental backlash be allowed.

Facebook has entrenched itself so deeply into the data economy that the harvesting, collection, and selling of data is more important to the company than the front-facing, public side of the company, which remains branded as a social media service. In reality, as Vaidhyanathan illustrates, "Facebook is the most pervasive surveillance system in the history of the world. More than two billion people and millions of organizations, companies, and political movements offer up detailed accounts of passions, preferences, predilections, and plans to one commercial service. In addition, Facebook tracks all of the connections and interactions among these people and groups, predicting future connections and guiding future interactions. It even compiles contact information on those who do not have a Facebook account" (Vaidhyanathan 57). Facebook is a data broker that uses connectivity and digital social interaction as a lure to entrap its laborers, who build data points that the company then claims as its own.

Amazon

Amazon is a giant of eCommerce, and their ventures into surveillance capitalism have been in pursuit of seamless, passive consumerism. The tech giant differs from other mentioned firms in its origins, mission, and financial model, but all the same, it has become tainted by the stink of the surveillance model.

Amazon was founded in 1994 by Jeff and MacKenzie Bezos. It began as an online bookseller operating out of a garage in Seattle. It would grow over the next few years, going public on the stock market in 1997. Struggling to compete against the established giants in the literature sector, Amazon set out to expand its operations in 1998 when it began selling CDs and DVDs, followed a few years later by clothing, appliances, electronics, and more.

From there the growth would not stop and the acquisitions would begin. In 2008, Amazon purchased Audible, an audiobook service, for $300 million, followed by Zappos, a competing online retailer, the following year for just shy of $900 million. As each year passed, Amazon's ambitions grew alongside its need for ever more capital (DePillis 2018).

It was that drive that led the company to look to a new market, an emerging sector that promised guaranteed returns as well as an optimization of their existing operations. Amazon was already familiar with the value of data from its retail origins. Using its position as a market-dominating commerce service, Amazon was able to accumulate a staggering amount of information on consumers' purchasing habits. In a 2019 article for *Cardozo Arts & Entertainment Law Journal*, Marc Veilleux Jr. explained this power, stating "Amazon’s biggest asset that permeates across its business lines is its trove of customer data, borne from years of an ever-increasing share of e-commerce sales. In 2009, Amazon captured fifteen percent of online spending; today, Amazon.com is the first place to search for products when shopping online for fifty-five percent of Americans" (Veilleux 496). Understanding both the power in data collection and the company's ability to invade new spaces and markets, Amazon set out to increase its data supply.

Amazon announced their entry into the surveillance market in 2014 when they launched the Amazon Alexa voice assistant device, staking their claim as a key figure in the 'Internet of Things' field, where appliances are equipped with internet capabilities, enhancing their functionality while also turning them into new data harvesters for the company. As of 2019, there were over 100 million Alexa devices sold (Lynskey 2019).

Just as Google laid claim to the streets with Google Maps, Amazon claimed its place in the household with the Alexa. The voice assistant was to serve as the digital butler for the everyday person, dutifully answering questions, completing tasks, and memorizing everything it heard, and reporting back to its corporate masters.

Understanding the murky nature of its surveillance apparatus, Amazon has invested heavily in ensuring its operations are not impeded by government oversight. According to an article published by Reuters, Amazon has constructed a governmental lobbying group consisting of roughly 250 employees. The article states that Amazon has "killed or undermined privacy protections in more than three dozen bills across 25 states" (Dastin 2021). This represents another key hurdle in the fight against surveillance capitalism. It has the money to protect itself, to influence politics and governance in its favor.

Where Amazon differs from the other tech firms is in its application of surveillance capitalism in its own operation. The company is unique from Facebook or Google in that it offers tangible products in addition to services. The eCommerce giant relies heavily on its retail shipping, which netted the company $53.2 billion in sales in the second quarter of FY 2021 (Reiff 2021).

In order to meet the demands of its global commercial shipping market, Amazon uses an array of technologies to maximize the productivity of its workforce. In Amazon fulfillment centers, workers are constantly monitored by an array of sensors and trackers. Each task they are given is accompanied by a time, the amount of time the algorithm has deemed the task should take. Failing to live to the standards of the algorithm can result in termination (Roosevelt 2021). Amazon delivery trucks are equipped with AI surveillance cameras that constantly monitor drivers, looking out for drowsiness, inefficiency, and recklessness (Vincent 2021).

Part 4: Logics of the Data Economy

In order to address the overarching crisis presented by the growth of surveillance capitalism, it is necessary to understand the fundamental mechanisms and logics that dictate its operation. The data economy is an economic network of information. Information is collected by data harvesting software, bought and sold by data brokers, and employed by algorithm developers to increase user engagements, in turn generating more information to be turned into data.

Algorithms

Predictive algorithm technology, as it is known today, was crafted at a young Google, looking to utilize the abundance of data collected from user search queries. Zuboff explains that "[Google] engineers and scientists were the first to conduct the entire commercial surveillance symphony, integrating a wide range of mechanisms from cookies to proprietary analytics and

algorithmic software capabilities in a sweeping new logic that enshrined surveillance and the unilateral expropriation of behavioral data as the basis for a new market form" (Zuboff 87).

While the systems were created with the motive of increasing the value of Google ad-space by improving click-through rates, the machine has far outgrown its humble beginnings. Ubiquitous computing in the modern era has allowed for algorithmic implementation in various facets of life.

The surveillance capitalist economy as seen today began with the promise of certainty. Google used its collected data and algorithmic analysis to target advertisements towards those most likely to engage with them, offering a new degree of certainty to prospective advertisers that shook the marketing economy to its core.

Algorithmic prediction tools are now employed across all major digital platforms. These content curation models display to the user not what they ask for, but what the platform believes will keep them engaged. The result is that content that elicits emotional reactions, such as anger or dissatisfaction, is disproportionality amplified on digital platforms. This is most evident in Facebook, where it was revealed that in 2017 the clickable reactive response indicating anger was weighed five times higher than a simple like response (Morrow 2021). The 'weight' of a digital reaction determines how much that response will increase the original post's visibility on other users' feeds. This resulted in posts containing controversial content getting placed on more users' pages. The ratio was altered in 2019, but not until three years of continued amplification of inciting content on the platform. Facebook's drive for maximum engagement has been the catalyst for a wave of misinformation and hate speech across the platform, leading to the amplification of conspiracy theories, disinformation, and violence.

The effects of increased platforming of inciting rhetoric cannot be understated. Facebook claims to be a force for egalitarian connection, but its policy indicates otherwise. The platform failed to curb calls for violence from supporters of Donald Trump following his unsuccessful Presidential reelection campaign, fueling the flames for the Capitol insurrection on January 6, 2021 (Riley 2021). In Myanmar, the platform was used to spread hate speech and lies, further complicating the ongoing humanitarian crisis occurring in the country, which the UN has labeled an 'ethnic cleansing' of the country's minority Muslim population (McKirdy 2018). In 2021, a former Facebook employee blew the whistle on the company, claiming before Congress that Facebook's engagement-based ranking was worsening violence in Ethiopia, which is in the midst of a civil war (Mackintosh 2021).

Facebook uses hate, fear, and anger to increase its data streams, and people die as a result. Fuchs writes that "algorithms and machines do not have ethics and morals. Data commodification means the emergence of new social inequalities, and intensifies the exploitative tendencies of the Internet" (Fuchs 59). The drive for data through algorithmic delegation is corrupting the internet and worsening world conflicts.

When a digital platform such as Google or Facebook employs a content algorithm to dictate what is shown to a user, they are exercising power over information access as well as crafting artificial perspectives for users to adopt. Users rely on digital platforms for news, knowledge, information, and more, and these platforms are determining which to show them and when based on the financial interests of the companies. When a user is only exposed to one type of content, whether it be news or entertainment, they are molded by only that perspective. In Jarion Lanier's book, *You are not a Gadget*, the father of virtual reality technology comments on

the impact of technology, highlighting the power of those in control of the dominant tech, stating that "technologies are extensions of ourselves… our identities can be shifted by the quirks of gadgets. It is impossible to work with information technology without also engaging in social engineering" (Lanier 4). In curating content through algorithms aimed at increasing engagement, Big Tech companies are exploiting the chemical stimulants of the human brain while inflicting damaging effects on those using their platform, generating the data that keeps them afloat.

This has resulted in a power imbalance that yields immense power to these platforms that face little to no meaningful regulations or oversight and craft values and ethics with marketing and image in mind. Vaidyanathan notes this regarding Facebook, stating that the "mix of the information we offer to Facebook, Facebook's ability to track us on the web and in the real world, and the commercial credit data it purchases empowers Facebook and disempowers us" (Vaidhyanathan 59). These companies, which were founded with high-minded philosophies of societal democratization and accessibility in mind, have become forces of decay for those very ideals.

Data

The narrative around data is rife with conflicting interests. Data, free from its potential for profit, is the digital trail left behind when individuals engage with online spaces. By the nature of computing, which relies on inputs to determine actions, the individual is constantly creating data points through their time spent online. Over a period of time, these data points add up. When fed through analytic mechanisms, data points can paint a picture of their creator - internets, habits, routines, desires, quirks, addictions, and so much more. When the analytic

mechanisms are deployed across a whole user base, social connections can be determined - friendships, lovers, rivals, enemies, business partners. All of this information is learned through the data points created by the users, harvested by the tech company in control of the platform.

Zuboff describes data as "the raw material necessary for surveillance capitalism's novel manufacturing processes. 'Extraction' describes the social relations and material infrastructure with which the firm asserts authority over those raw materials to achieve economies of scale in its raw-material supply operations" (Zuboff 65). The value of data amplifies exponentially in scale, since analytic systems grow more accurate the more data they encounter. This is why Big Tech companies gobble up startups and competitors, shelling out monetary figures far higher than the smaller companies' true value. What the Big Tech companies actually are purchasing is the data stream, an untapped user base that promises to pump out resources previously out of reach, as well as the already collected data.

In order for the data-based surveillance economy to operate uninhibitedly, the tech companies need for the logics of data to not be fully understood. The narrative so meticulously crafted is that data is akin to engine exhaust, a side effect, an afterthought that happens to be produced when humans clash with technology. This narrative allows for the tech companies to claim the data for themselves without compensating those whose efforts and labor generated the data.

The dominating counter-argument at present is that users are compensated through access to the service, and their data is the price of usage. While this is a true statement, it is not a sound argument and not the basis for a healthy economy or society. Economic transactions can not be clouded in disproportionate secrecy, and this is the case with data harvesting. Users are not

adequately informed of the tech companies' data collection practices. If these methods are public at all, they are buried inside strategically bloated terms of service agreements. Tech companies' practices and efforts to hide their data collection methods are proof that this is not a fair goods-and-services exchange. If digital platforms want this to be the tradeoff users agree to in order to access the online service, there must be transparency regarding what data is being collected, who has access to it, who has the ability to purchase it, and how long the company will retain the data.

Data are digital packets of information generated through human engagement with online spaces. In the present information economy, data has become commodified. However, that commodity has not yet been fully realized for what it is. Were this to happen, it would stand to reason that those laboring to create the commodity would be compensated for their labor, not exploited.

In an attempt to recalibrate societal understanding of data, and the way in which its collection and extraction are altering both global economies and social relations, scholars have increasingly drawn links between the data economy and historical colonial practices, coining the term "data colonialism," with scholars Nick Couldry and Ulises A. Mejias writing that "while the modes, intensities, scales and contexts of dispossession have changed, the underlying drive of today’s data processes remains the same: to acquire 'territory' and resources from which economic value can be extracted" (Couldry 3). While the exploitation of data colonialism is far less gruesome and inhumane than the institution from which it gets its name, it is nevertheless a system constructed around an ideology of power, exploitation, profit, and social reconfiguration.

The scholars emphasize that the manner in which data economies are understood determines the ways in which their ugly elements are resisted and made livable. "Recognising

what is happening with data as a *colonial* move means acknowledging the full scope of the resource appropriation under way today through datafication: it is human life itself that is being appropriated so that it can be annexed directly to capital as part of a reconstruction of the very spaces of social experience" (Couldry 2). The impact of the data economy cannot be understated.

Not only is data colonialism altering economic markets and recalibrating human relations, but it is turning the direction of technological advancement in a direction that serves the system of data extraction, just as technological systems in the colonial era were crafted with labor exploitation, resource extraction, and trade in mind.

Part 5: Resistance to Surveillance Capitalism

Regulatory approaches to surveillance capitalism with a framework of monopoly busting are too narrow minded to address the issue. The problem is not so much the companies at the top, although they deserve no shortage of condemnation and blame, but the emerging market and economic imperatives driving the actions of the companies.

Calls for regulation on Big Tech are increasing but not nearly as fast as the companies are growing and expanding their operations. Recent years have seen an increase in discussions in Washington, specifically, regarding clamping down on Big Tech, but political divisions are fracturing the regulatory push. On the Democrat side, pro-regulation lawmakers are seeking to hold tech companies like Facebook accountable for misinformation and hate speech posted and propagated on their platform. On the other side of the aisle, Republican lawmakers are approaching the issue in their usual fashion by making themselves the victim, claiming that social media companies are censoring conservative voices (Kang 2021). Despite both parties

agreeing that tech companies need to be reigned in, they are unable to come to a consensus regarding which elements of the companies, real or fictional, to address and regulate.

This division is compounded by a staggering amount of technological illiteracy among United States lawmakers. When Mark Zuckerberg testified before a Senate committee in 2018, committee members were unable to properly question the Facebook CEO on matters of privacy and data because they lacked knowledge of the logics of basic technology, much less surveillance capitalism (Byers 2018). What resulted was a plethora of soundbites of Mark Zuckerberg struggling to explain basic technological procedures to a panel of disgruntled geriatrics.

While recent hearings on Big Tech, such as a whistleblower testimony from a former Facebook data scientist (Allyn 2021), show improvement in lawmakers' efforts to understand the technology they are looking to regulate, they still lack the intellectual power to combat the Silicon Valley juggernauts.

In order for Congress to properly craft legislation that addresses the problems with Big Tech and the data economy, representatives must be informed of what the problems are, what is causing them, and how they can be curtailed. One proposed solution is to bring back the Office of Technological Assessment. The OTP was created for exactly this purpose, consisting of a team of experts with knowledge on science and technology ready to advise Congress. One reason the current Congress approaches these testimonies with so little understanding of the technology is that this office does not exist anymore, killed in a round of budget cuts two decades ago (Zetter 2016). Bringing back this office could result in better-informed, better-equipped lawmakers who can properly address the problems they currently only marginally comprehend.

Couldry and Mejias write that "society-wide responses are needed to such society-wide transformations" (Couldry 5). Campaigns to delete Facebook accounts do well to shed light on the issues present in the surveillance capitalist system, but the data economy is too far-reaching and powerful to be impacted by individual actions such as this.

State action through policy and economic sanctioning is the most effective way Big Tech companies can be dissuaded from their continued adherence to and adoption of imperatives of surveillance capitalism. Public outcry is bad for these companies, no question, but all it takes to counter this is an increase in funding to their branding and marketing departments. Image can be remedied with time and effort. The most effective way to inflict damage on data extracting companies is to hit them in the only place they care about: their wallets.

The Myth of Self-Regulation

The long-standing argument of tech companies is that they are capable of self-governance on their platforms. Facebook, Twitter, and others claim exception from responsibility for hate speech and misinformation amplified on their platform but claim they are taking action to combat such content. Their logic and methodology are inefficient, however, because they are only capable of tackling issues from inside the confines of the economic imperatives dictating their operations.

The result is a game of cat and mouse, where platform moderators hopelessly stamp out dangerous content they come across but never address the issues that are allowing that content to emerge. This is because the platforms' algorithms and policies are the problems. If the

moderators were operating outside of the financial interests of the tech firm, the solution would be clear - reform the platform - but this is not what the platforms are truly looking to do.

As concerns of privacy and data collection have become more common in the consumer space, tech companies are looking for ways to ease fears. However, the goal of the surveillance capitalists is clearly to subdue users into a false sense of security, not to actually ensure privacy protections. This is most evident with Apple's recent privacy update, which allows users to 'ask' third party apps not to collect data from their device. The rollout of this new feature was heralded with a glitzy marketing campaign ensuring users of Apple devices that the company was prioritizing privacy and resistance to tracking. It quickly became clear, however, that this feature was mostly performative and did little to prevent tracking (Towey 2021).

Tech firms can not be trusted to govern their own privacy standards when they have constructed their entire business model around invasion. They can only offer false hope, performative resistance, and lies. Only an outside force without capital investment in the mechanisms of surveillance capitalism can dismantle the operation.

Algorithm Policy

Algorithms have caught the eye of United States policymakers more so than any other logic of surveillance capitalism.

In March 2021, New Jersey Congressman Tom Malinowski and California Congresswoman Anna G. Eshoo reintroduced the Protecting Americans from Dangerous Algorithms Act, which, if passed, would amend Section 230 of the Communications Decency

Act to "remove liability immunity for a platform if its algorithm is used to amplify or recommend content directly relevant to a case involving interference with civil rights"

In a statement regarding the bill, Congressman Malinowski said that

> "social media companies have been playing whack-a-mole trying to take down QAnon conspiracies and other extremist content, but they aren't changing the design of a social network that is built to amplify extremism. Their algorithms are based on exploiting primal human emotions — fear, anger, and anxiety — to keep users glued to their screens, and thus regularly promote and recommend white supremacist, anti-Semitic, and other forms of conspiracy-oriented content. In other words, they feed us more fearful versions of what we fear, and more hateful versions of what we hate. This legislation puts into place the first legal incentive these huge companies have ever felt to fix the underlying architecture of their services — something they've shown they are capable of doing but are consciously choosing not to." ("Reps. Malinowski and Eshoo Reintroduce Bill to Hold Tech Platforms Accountable for Algorithmic Promotion of Extremism 2021)

The bill aims to amend Section 230 of the Communications Decency Act, which grants legal immunity to digital platforms for the content posted by users on their websites. The amendment would add an exception to this immunity that would allow for tech companies to be held liable for violence-inciting content that is promoted by the platform's content algorithms. This is one of a handful of proposed bills looking to change Section 230, but at present it seems the moderate wings of both parties will keep such legislation from inaction, citing fear of governmental overreach.

Data Policy

The strongest enacted legislation combating data extraction comes from the European Union, which passed the Grand Data Protection Regulation (GDPR) in 2018. The legislation requires all companies with business in the European Union, domestic or international, to meet a level of compliance with the act under penalty of fines. The restrictions outlined in the principles of the GDPR strike at the most crucial mechanisms of the data economy, written in a manner vague enough to address the vast reaches and interests of Big Tech companies.

Under the GDPR, data extracting companies must be transparent regarding their extraction operations to their users, must have a clear purpose for extraction, must only extract the minimum data required to serve the said purpose, and must store data for only as long as needed for that purpose. Companies are also on the hook for ensuring the security and confidentiality of the data they collect.

Also included in the GDPR is a bill of rights specifically pertaining to subjects of data extraction, these being: the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, rights in relation to automated decision making and profiling (“What Is GDPR, the EU's New Data Protection Law?” 2019).

Since the Grand Data Protection Regulation passed, regulators have fined Big Tech companies over 800 times (“GDPR Fines List: Find All GDPR Fines & Detailed Statistics.”), with the largest penalty to date being levied at Amazon, which was fined $888 million in July of 2021 for processing personal data in violation of the GDPR (Kaur 2021).

However these fines, while sizable, are not effectively dissuading websites from engaging in invasive practices, as seen by a study conducted by researchers from the University of Virginia, which concluded that 97% of websites violate at least one of the restrictions outlined in the GDPR (Anderson 2021). At present, fines are simply seen as the cost of doing business in the lucrative European market. Until fines are so financially damaging that they outweigh the profits of surveillance capitalism, practices will not change.

Before concluding this paper, readers are encouraged to take part in one last exercise, carefully designed to convey the fundamental message of the essay.

Exercise 3

Required materials: Bamboo finger trap (also known as a Chinese finger trap or Chinese finger puzzle), social skills, the gift of observation.

Instructions: Over the course of a day, ask a number of people to stick their index fingers into each end of the finger trap. Ideally, select people with no prior knowledge of the trap. Watch and observe the methods used to escape, successful and unsuccessful.

Watch as they tug and pull their fingers apart, only resulting in the trap tightening, constricting around their fingers. They may struggle with this for some time. The most common initial strategy will be to use brute strength to overpower the bamboo lacing. This may work for some, but most will only wear themselves out.

The ones who succeed will be the ones who take a moment to analyze the composition of the trap. They will observe that when they pull their fingers apart, the trap is pulled too, causing it to tighten further as the bamboo weaving constricts from the tension.

In order to escape the trap, they have to do the opposite of their first instinct. They will push their fingers together, deeper into the trap. This will alleviate the tension in the bamboo weaving and cause the trap to loosen. From here, they can simply pinch the trap with their middle finger and thumb and easily remove their fingers.

In order to effectively deconstruct something, you must understand how it was constructed.

Conclusion: Cutting the Legs off of the Data Economy

The way to fight surveillance capitalism is to understand its mechanisms. For too long, tech companies have benefited from the ignorance of their user base. It's impossible for someone to resist a force they do not understand. By shining a light on the logics of surveillance capitalism and understanding the negative consequences of the data economy, steps can be taken to dismantle the economic imperatives dominating these companies.

The fights worth fighting are often the long ones. Surveillance capitalism will not be dismantled as fast as it was created. The forces aiding it are well-financed, well-defended, and well equipped.

But the integrity of the Internet is worth fighting for. Humans have just begun to scratch the surface of what is possible when they are all on the same page, and the Internet is a tool to achieve that dream. In order to preserve the grand potential of computing, there must be a

recalibration of technology's role in society. Will it continue as a tool for profit or change into a tool for good?

This course correction will only come to fruition if a sizable portion of Internet users are educated on the mechanisms of surveillance capitalism. As the much talked about dawn of Web 3.0 approaches, tech firms have a new opportunity to capitalize on technological ignorance among their user base, allowing for invasions of privacy to not only occur uninhibited, but unseen altogether.

For the average Internet user, there is no effective way to curb surveillance capitalism at present. This is not cause for complacency, however, but instead a call to action. The first step of resistance is education. Tech firms must be forced into transparency regarding their data collection mechanisms. There is room for optimism in this regard, most notably the announcement of the PATA Act (Platform Accountability and Transparency). The bipartisan bill would require tech firms to share platform data with researchers under threat of losing section 230 exemptions (Faife 2021). Should this bill be passed and properly enforced, the ugly elements of surveillance capitalism, which tech firms have long fought to keep shrouded, could be brought to light.

In choosing to fight the drives of surveillance capitalism, to push back against malignant forces corrupting the Internet, there is a conscious decision to go against guaranteed profit. In a free market, capitalist economy, this is a radical notion. But should the discussion be separated from the debilitating lens of capitalism, a future can be seen far preferable to the present course. First, this future must be imagined. Second, the current system must be dismantled.

Sources

Al-Abbas, Linda S., et al. “Google Autocomplete Search Algorithms and the Arabs’ Perspectives on Gender: A Case Study of Google Egypt.” *GEMA Online Journal of Language Studies*, vol. 20, no. 4, Nov. 2020, pp. 95–112. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=edo&AN=147725447&site=eds-live.

Allyn, Bobby. “Here Are 4 Key Points from the Facebook Whistleblower’s Testimony on Capitol Hill.” *NPR*, 5 Oct. 2021, www.npr.org/2021/10/05/1043377310/facebook-whistleblower-frances-haugen-congress.

Anderson, Martin. “AI Researchers Estimate 97% Of EU Websites Fail GDPR Privacy Requirements- Especially User Profiling.” *Unite.AI*, 26 Nov. 2021, https://www.unite.ai/ai-researchers-estimate-97-of-eu-websites-fail-gdpr-privacy-requirements-especially-user-profiling/.

Byers, Dylan. “Senate Fails Its Zuckerberg Test.” *CNNMoney*, 10 Apr. 2018, money.cnn.com/2018/04/10/technology/senate-mark-zuckerberg-testimony/index.html.

Cho, J., et al. *Do Search Algorithms Endanger Democracy? An Experimental Investigation of Algorithm Effects on Political Polarization*. 2020. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=edssch&AN=edssch.oai%3aescholarship.org%2fark%3a%2f13030%2fqt9dr6q639&site=eds-live.

Couldry, Nick and Ulises A. Mejias. "Making data colonialism liveable: how might data’s social order be regulated?". Internet Policy Review 8.2 (2019). Web. 30 Oct. 2021.

Dastin, Jeffery, et al. “The Amazon Lobbyists Who Kill U.S. Consumer Privacy Protections.” *Reuters*, 19 Nov. 2021, www.reuters.com/investigates/special-report/amazon-privacy-lobbying/.

DePillis, Lydia, and Ivory Sherman. “Amazon’s Extraordinary Evolution: A Timeline.” *Cnn.com*, CNN, 4 Oct. 2018, www.cnn.com/interactive/2018/10/business/amazon-history-timeline/index.html.

Faife, Corin. “New Social Media Transparency Bill Would Force Facebook to Open up to Researchers.” *The Verge*, 10 Dec. 2021, www.theverge.com/2021/12/10/22827957/senators-bipartisan-pata-act-social-media-transparency-section-230. Accessed 11 Dec. 2021.

Fuchs, Christian. “Karl Marx in the Age of Big Data Capitalism.” *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data*, 2019, pp. 53–71., https://doi.org/10.16997/book29.d.

“GDPR Fines List: Find All GDPR Fines & Detailed Statistics.” *Privacy Affairs*, 25 Feb. 2021, https://www.privacyaffairs.com/gdpr-fines/.

Greenwald, Glenn and MacAskill, Ewen. "NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. 7 Jun. 2013. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Horvath, Sarah. “The History of Google Stock & Google Stock Split • Benzinga.” *Benzinga*, 24 Mar. 2021, www.benzinga.com/money/history-google-stock/. Accessed 1 Dec. 2021.

Johnson, Joseph. “Google Sites: Advertising Revenue 2020.” *Statista*, 5 Feb. 2021, https://www.statista.com/statistics/266242/advertising-revenue-of-google-sites/.

Jones, Campbell, et al. *For Business Ethics*. Routledge, 2005. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=cat05467a&AN=ecl.2218689&site=eds-live.

Kang, Cecilia. "Lawmakers See Path to Rein in Tech, but It Isn't Smooth." *The New York Times*, 2021, www.nytimes.com/2021/10/09/technology/facebook-big-tobacco-regulation.html. Accessed 1 Dec. 2021.

Kaur, Dashveenjit. "Amazon Slapped with Biggest GDPR Data Privacy Fine, Ever." *TechHQ*, 2 Aug. 2021, https://techhq.com/2021/08/amazon-slapped-with-biggest-gdpr-data-privacy-fine-ever/.

Lanier, Jaron. *You Are Not A Gadget: A Manifesto*. Vintage Books, 2011.

Lynskey, Dorian. "'Alexa, Are You Invading My Privacy?' – the Dark Side of Our Voice Assistants." *The Guardian*, The Guardian, 9 Oct. 2019, www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants.

Mackintosh, Eliza. "Facebook Knew It Was Being Used to Incite Violence in Ethiopia. It Did Little to Stop the Spread, Documents Show." *CNN*, Cable News Network, 25 Oct. 2021, https://edition.cnn.com/2021/10/25/business/ethiopia-violence-facebook-papers-cmd-intl/index.html.

Maruf, Ramishah. "Researchers Studying FACEBOOK Misinformation Say They Were Deplatformed." *CNN*, Cable News Network, 5 Sept. 2021, https://edition.cnn.com/2021/09/05/media/reliable-sources-facebook-researchers-deplatform/index.html.

McKirdy, Euan. “When Facebook Becomes 'the Beast': Myanmar Activists Say Social Media Aids Genocide.” *CNN*, Cable News Network, 7 Apr. 2018, https://edition.cnn.com/2018/04/06/asia/myanmar-facebook-social-media-genocide-intl/index.html.

Morrow, Brendan. “Facebook Reportedly Gave the Angry Emoji 5 Times as Much Weight as a 'like'.” *The Week*, The Week, 26 Oct. 2021, https://theweek.com/facebook/1006422/facebook-reportedly-gave-the-angry-emoji-5-times-as-much-weight-as-a-like?amp.

Pilkington, Ed. "'Panic made us vulnerable': how 9/11 made the US surveillance state - and the Americans who fought back." *The Guardian*. 4 Sep. 2021. https://www.theguardian.com/world/2021/sep/04/surveillance-state-september-11-panic-made-us-vulnerable.

Reid, Kris. “Google Search Statistics: How Many Searches per Day on Google in 2021 ?” *Ardor SEO*, 27 June 2021, https://ardorseo.com/blog/how-many-google-searches-per-day/.

Reiff, Nathan. “How Amazon Makes Money: Cloud Services Takes Off.” *Investopedia*, 5 Feb. 2021, www.investopedia.com/how-amazon-makes-money-4587523.

“Reps. Malinowski and Eshoo Reintroduce Bill to Hold Tech Platforms Accountable for Algorithmic Promotion of Extremism.” *Representative Tom Malinowski*, 24 Mar. 2021, https://malinowski.house.gov/media/press-releases/reps-malinowski-and-eshoo-reintroduce-bill-hold-tech-platforms-accountable.

Riley, Michael. “Facebook Faulted by Staff Over Jan. 6 Insurrection: ‘Abdication.’” *Bloomberg.com*, Bloomberg, 22 Oct. 2021, https://www.bloomberg.com/news/articles/2021-10-22/facebook-faulted-by-staff-over-jan-6-insurrection-abdication.

Roosevelt, Margot. "'The Algorithm Fired Me': California Bill Takes on Amazon's Notorious Work Culture." *Tech Xplore - Technology and Engineering News*, 31 Aug. 2021, techxplore.com/news/2021-08-algorithm-california-bill-amazon-notorious.html.

Silverman, Jacob. "Privacy under Surveillance Capitalism." *Social Research*, vol. 84, no. 1, Mar. 2017. *EBSCOhost*, search-ebscohost-com.proxy.emerson.edu/login.aspx?direct=true&db=edsbig&AN=edsbig.A518533190&site=eds-live.

"Surveillance under the USA/Patriot Act." *American Civil Liberties Union*, https://www.aclu.org/other/surveillance-under-usapatriot-act.

The Constitution of the United States: A Transcription. *National Archives*, U.S. National Archives and Records Administration, 1 Dec 2021, https://www.archives.gov/founding-docs/bill-of-rights/what-does-it-say.

"The Fallout of Edward Snowden and His Leaked Documents, Eight Years Later." *AXEL.org - Bringing Awareness to Data Custody*, AXEL, 11 Aug. 2021, https://www.axel.org/2021/07/16/the-fallout-of-edward-snowden-and-his-leaked-documents-eight-years-later/.

Towey, Hannah. "Former Apple Engineer Says the Button on IPhones Asking Apps Not to Track You Is a 'Dud' That Gives Users a 'False Sense of Privacy'." *Business Insider*, Business Insider, 24 Sept. 2021, https://www.businessinsider.com/apple-iphone-privacy-initiative-ask-app-not-to-track-study-2021-9.

Veilleux, Marc J., Jr. "Alexa, Can You Buy Whole Foods: An Analysis of the Intersection of Antitrust Enforcement and Big Data in the Amazon-Whole Foods Merger." *Cardozo Arts & Entertainment Law Journal*, vol. 37, no. 2, Jan. 2019, pp. 481–512. *EBSCOhost*,

search.ebscohost.com/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.caelj37.20&site=eds-live.

Véliz, Carissa**.** "Why We Should End the Data Economy." *The Reboot*, 10 June 2021, thereboot.com/why-we-should-end-the-data-economy/.

Vincent, James. "Amazon Delivery Drivers Have to Consent to AI Surveillance in Their Vans or Lose Their Jobs." *The Verge*, 24 Mar. 2021, www.theverge.com/2021/3/24/22347945/amazon-delivery-drivers-ai-surveillance-cameras-vans-consent-form.

"What Is GDPR, the EU's New Data Protection Law?" *GDPR.eu*, 13 Feb. 2019, https://gdpr.eu/what-is-gdpr/?cn-reloaded=1.

Zetter, Kim. "Of Course Congress Is Clueless about Tech—It Killed Its Tutor." *Wired*, 21 Apr. 2016, www.wired.com/2016/04/office-technology-assessment-congress-clueless-tech-killed-tutor/. Accessed 2 Dec. 2021.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: the Fight for a Human Future at the New Frontier of Power*. PublicAffairs, 2020.