Surveillance Capitalism and Democracy: Intersections of Epistemic Injustice

By
Zac Toni

Submitted to
Central European University
Department of Political Science

In partial fulfillment of the requirements for the degree of Master of Arts in Political Science

Supervisor: Professor Zoltan Miklosi

Vienna, Austria
(2021)

Abstract:

The pervasiveness of Big Data has become inescapable and in the 21st century it has become the *magnum opus* of surveillance and surveillance capitalism. With the omnipresence of datafication and dataveillance today, algorithms have become a new form of informational power facilitating the shift from enclosed structures to entangled systems of knowledge, power, and authority. Accordingly, how does the capitalist surveillant-assemblage affect democracy in the context of changing identities and digitized class relations? The objective of this paper is to analyze how sweeping engagement with search engines and social media alters individual and group identities and agency; and to uncover how these alterations establish new forms of epistemic injustice, particularly in relation to democracy. For liberal democracy to flourish there must be a network of intermediary institutions which enable individuals to get information and inform their judgement. However, the current operational design of social media databases deteriorates and fragments such institutions, making it more difficult to understand both ourselves, others, and a common world. Overall, the status quo of algorithmic social profiling by social media poses a serious threat to citizens' ability to freely interpret political realities and their ability to understand a reasonably common political world.

Table of Contents

Introduction

In 2010 the CEO of Google, Eric Schmidt proclaimed that more information was produced on the internet every 48 hours than between the beginning of civilization and 2003, five Exabytes (or five billion Gigabytes). By 2025, it is expected that 463 exabytes will be produced on the internet daily (SeedScientific 2021). Today, cyberspace has penetrated nearly all facets of society from the global knowledge-economy to human agency and identity. This information and communication technology (ICT) revolution is constitutive of a new human socio-cultural environment that blurs the boundaries between online and offline life. Datafication has led to a remarkable optimization of diverse critical processes from bookkeeping efficiency, digital surveillance, to epidemiological research. From disinformation campaigns, algorithmic discrimination, hate speech promulgation, to discrete social categorization and biopolitics- these diverse datafication processes represent a substantial shift in social structure, human agency and identity, as well as capitalistic power asymmetries. As computer networks became the central infrastructure for virtually all facets of society, implying a "massive immersion of our cognitive life in digital environments" (Scotto 2020, 152), scholars have begun to denote this fluid situation as the digital condition (Scotto 2020, 151). This emergent digital age necessitates a critical inquiry to the digital condition's implications for human agency and identity, socio-cultural shifts, and the realm of politics. The internet emerged with libertarian utopian visions including the democratization of information, the empowerment of disenfranchised voices, and the increase and outsourcing of cognitive capacities; all of which pointed to the augmentation of human agency and autonomy.

On the contrary, it has become evident that technological development left unchecked can easily diminish the democratic capacity and accountability of both individuals and groups. Briefly, the internet reigned in a new socio-economic paradigm, the context and operation of this paradigm is why social media datafication can no longer be implicitly characterized as neutral or innocent technologies of emancipation. Scholars from various disciplines of social science have now begun to call this socio-economic paradigm *Surveillance Capitalism*, a system that "unilaterally claims human experience as free material for translation into behavioral data" (Zuboff 2016, 14); this commodification of human experience relies on behavioural predictability and must modify human behaviour as a condition of success (Zuboff, 353). With this in mind, is the digital revolution obligating democracies to reconsider the moral and political rules of behaviour that regulate agreements between citizens, corporations, and governments? More specifically, how does the capitalist surveillant-assemblage affect democracy in the context of changing identities and digitized class relations?

Today, surveillance capitalists have methodically exploited a delay in social evolution as the swift advancement of their abilities to surveil for profit elude social understanding and policy adaptation (Zuboff 2019, 83). The centrality of this exploitation emerges from the intelligent designs of these datafication systems, these are machine intelligence systems that are designed to be unknowable by the user. That is to say, the inputs and outputs can be inquired upon while the inner operational processes are structurally out-of-sight; this is known as a 'black box' algorithm. A 'black box' is "anything having a complex function that can be observed but whose inner workings are mysterious or unknown" (Collins Dictionary 2021). By design, the black-box science of social media datafication hinders our socio-political self-understanding. The

opaqueness of these data operations alongside each platform's behavioural inputs and outputs inherently complicates inquiries of informational power dynamics. This means that it is notoriously difficult to recognize whether social media shapes political attitudes or whether political attitudes shape social media. What is clear however, is that polarization and partisanship has been rising in the U.S. since the 1970s, and rapidly since the 2000s (Grumbach 2018). As will be noted, this polarization has been marked by asymmetry especially among right-wing media sources and conservative epistemic communities. This rapid increase and asymmetry of polarization since the Web 2.0 boom calls for further inquiry into the feedback loops of social media and the epistemic logic of surveillance capitalism.

The field of critical digital studies has emerged as a highly interdisciplinary field drawing upon many avenues of the social science and humanities canon(s). The competing understandings of ICTs have entangled the discipline with a tension between divergent analytical approaches from lenses of Marxism, social cognitive theory, and various postmodern frames. What each of these approaches has in common regarding Surveillance Capitalism is the (typically indirect) implication of epistemic cleavages on human capacities and particularly those capacities which are building blocks of democracy. However, few of these approaches place any overt primacy on the perspective of epistemic injustice. The problem with this is that informational power becomes a periphery to the dominant discourses of digital surveillance. The issue at hand is not particularly about ‘good’ or ‘bad’ actors of social media platforms, the issue stems from the socioeconomic *logic* of surveillance markets. This logic compels Big Data platforms to establish institutional designs of datafication that do not recognize social media as an inherently political

sphere. Granted that, the lens of epistemic injustice is a promising avenue to dissect the *particulars* of social media to the *general*(*s*) of surveillance capitalism.

The objective of this paper is to analyze how sweeping engagement with search engines and social media alters individual and group identities and agency; and to uncover how these alterations establish new forms of epistemic injustice, particularly in relation to democracy. For liberal democracy to flourish there must be a network of intermediary institutions which enable individuals to get information and inform their judgement. However, the current operational design of social media databases deteriorates and fragments such institutions, making it more difficult to understand both ourselves, others, and a common world. This analysis will focus upon the North American context. Overall, the status quo of algorithmic social profiling by social media poses a serious threat to citizens' ability to freely interpret political realities and their ability to understand a reasonably common political world.

Chapter 1: A Memoir of Digital Identity

I received my first cell phone in grade 7 at the age of twelve, it was a Samsung SPH-M300, a very basic and low-budget flip phone. I was beyond thrilled to have my own cell phone, however, in looking back on this excitement, it was not simple to remember why I was so excited. At first, I thought that my excitement was based on the idea of essentially limitless connectivity; perhaps this was one aspect. I have come to realize that my excitement over my first cell phone was part of an unfolding Western ethos in which digital technology is a key pillar of identity. Obtaining a cell phone has become one of the most palpable rites of passage to adulthood in middle- and upper-class households across Canada and much of the West. Upon reflection, it is glaring that the cell phone was the first obvious symbol of transition from child to adolescent. The cell phone is a symbol of adulthood insofar that it comes with several rights and responsibilities. The primary reason my parents would pay for one was so that they could keep tabs on me, to make sure I was safe and not up to trouble. So, I had a verbal contract to check in with my parents at set times each day and a responsibility to not use more talk-minutes than my plan allowed. There was also an aspect of peer pressure at play in how I wanted a cell phone. To not have a cell phone by around grade 7 or 8 was considered strange or abnormal. If you did not have a cell phone, the other children would certainly inquire as to why 'your parents would not let you'. Is your family super religious? Are your parents strict? You know they aren't that expensive right? These are all common questions children would ask in addressing the 'oddness' of peer unconformity.

When I received my first cell phone in grade 7 I was certainly one of the last in the class to have received one; typically, classmates would have gotten theirs in grade 6 or early grade 7. Interestingly, it seems that in 2021 this acquisition of a cell phone has moved on to even younger

grades, to even those as young as grade 3. As a result, it seems difficult to tell if a child's first cell phone will continue to be such a rite of passage as children continue to acquire cell phones at younger ages. This is a conspicuous example of how "certain styles of technological attachment become dominant in particular places and times; examining individual relationships with technology can be a window onto larger social forces" (Turkle 2011, 18).

Eventually (today even), children may receive their first cell phone at such a young age that the phone could no longer be perceived as a rite of passage to adolescence. However, what seems more telling is the larger picture that the modern era, largely characterized by digital technology, will be marked by a series of 'technological transitory rites of passage'. However, it is significant to note that the cellular rite of passage was never truly a static ritual. My first cell phone could send and receive text messages and calls, view a calendar, and a type in a notepad. In contrast, today's smartphones can do nearly anything a laptop or desktop computer can do. The cell phone has gone from talk and text connectivity of close friends, towards a coalescence of nearly all digital mediums: mp3 player, fitness tracker, search engine, camera, arcade machine, and social media powerhouse, all in one. This has happened in less than a decade. Psychoanalyst Erik Erikson writes of adolescence as a time of moratorium, meaning a time of passionate experimentation and interaction with new people and ideas; time in cyberspace reshapes the notion of the moratorium because it exists as an ongoing activity (Turkle 2011, 20). The possibility to be online at any time and place of day is consequently altering our sense of what it means to be together.

During the age of around 12, my tense relationship with a friend became exacerbated by social media (Most details are left out here or vague, purposely out of respect). Throughout the age of 12-18 I sent him several friend requests on Facebook, all of which were declined. Unfortunately, my friend had very bad social anxiety which has caused him to move schools over lack of friends. It seemed that the only group that would truly accept him were the mischievous 'punk-rock' type crowd entangled with drug users and sellers. Many nights I remember he would not come home and my and his family were obviously worried sick. He would often leave for several days (even weeks) at a time, unannounced. Understanding of this situation only began once we saw his social media. One time he went missing for a week when we were 14 and in an effort to discover his whereabouts, we hacked into his Facebook through figuring out his security question to recover the password. Everything began to make sense after this. My friend had developed a virtual identity as a 'gangster' (for lack of a better term). My friend's social anxiety was at one time saved by social media, and at other times deeply hurt. He decided that a new identity could bring him friendship; and he was right to an extent. However, social media proved to be much more divisive than inclusive, as no family members (nor school 'friends') were permitted to view his social media profile(s). He was uncomfortable in his identity and decided to create a new one, virtually. His online 'gangster' identity manifested into his offline identity. In other words, the online and offline became one in the same. Today, after a long, bumpy road of addiction and rehabilitation, he is doing well and is becoming a nurse and we now have a great relationship. This reflection of my upbringing along with my friend has shown how modern digital technology has truly become inseparable from 'offline' identity.

Moreover, the modern-day smartphone has given rise to a remarkably dialectical relationship with my identity. The standard narrative of the smartphone is that of connectivity. However, the smartphone in my life has also come to be a symbol of reclusiveness. The scenario of myself on a bus staring down at my iPhone with my headphones in, is analogous to the 'do not disturb' sign available in hotel rooms. The smartphone has seemingly become a sort of modern-day spellbinding of attachment to the self insofar as the use of my smartphone is often highly subconscious. For example, many will often aimlessly scroll through social media feeds without particularly reading or observing much of what is being shown on the screen. It is a sort of hypnotic fear of missing out, or perhaps a subliminal connection to the digital cloud which presents comfort and satisfaction.

Everyday individuals routinely check social media and the news on their smartphone within minutes of waking up, and probably another 10 times throughout the day before checking again before bed. Most nights it has become commonplace to aimlessly scroll through social media before bed, perhaps out of boredom; however, many do this even though they are fully aware that staring at a screen right before bed can make it difficult to sleep. This scrolling is addictive insofar as it is difficult to moderate, even when it results in insomnia woes. This scrolling of news and other social media through smartphones is truly representative of how much learning and knowledge, in a receptive sense, is outsourced to the digital environment. In the end, it seems the smartphone has become a highly dialectical extension of the self insofar as its powers and capabilities have had a layering effect of contradictions upon identity. The smartphone is at one time socially cohesive, and at other times highly conducive to reclusiveness. The smartphone

is certainly a prosthetic of the self insofar as much of one's learning is outsourced to it; and a sense of knowledge-loss is felt when it is inaccessible.

Chapter 2: Operations, Regulations, and Technology of Surveillance

2.1 Surveillance Technology

The focus of surveillance operations in this paper is focused solely on web-browsing for it is the preeminent surveillance mechanism today. How are governments or businesses able to use collected data from a requested online search to find out what you have been searching? The answer is typically via 'cookies' and IP addresses. Every computer and smartphone that accesses the internet holds a unique IP address; an IP address allows you to surf information on the web and allows that information to track back to you, subsequently, making it possible to identify and locate a user similar to a home address in a phone directory. 'Cookies' were invented in 1994 so that information could be saved between visits to a website:

> A cookie is a small piece of text that is placed on a user's computer when visiting a website. Cookies can be used to track what sites users visit and what they do on them. From this information, third parties, such as advertisers, can build profiles of users that can then be used to place specific advertisements on the websites those users visit. (Office of the Privacy Commissioner, 2017)

Cookies are the key surveillance technology of web browsing and every popular website uses them, and without them users would have minimal website functionality. Cookies have their share of benefits such as saving your general interface settings including your login information. However, one of the primary issues with cookies is that they are often applied to users' computers without their knowledge or consent. 'Third party cookies' are organizations not directly involved in the interaction between the user and the website, most commonly being advertising companies who mine the behavioural data from these cookies to target their advertisements.

Adobe's popular Flash browser add-on has now created a mechanism called 'Flash Cookies' (also known as Local Shared Objects or LSOs) which are similar to traditional web Cookies

except they are highly resilient. If you delete traditional web Cookies, Flash Cookies can be applied to recreate them. Flash cookies are also significantly more hidden than traditional web cookies and consequently quite difficult to remove. 'Super Cookies' utilize a new storage location of Web 2.0 built into browsers to save personal information, making their storage functionality much greater and more flexible than traditional web Cookies. Altogether, users often have no knowledge of when any of these cookies are being used and they are often not given mechanisms to control this information. Websites also use tools called "filter bubbles" that choose depending on the data predictions of different variables (sometimes dozens or hundreds) that is the content related to the ideas, prejudices, and interests of the users' (Scotto 2020, 172); these categorizations allow social networks to keep the ones that think alike us near, and far from those who think different, segregating and marginalizing epistemic communities.

Google's privacy policy page begins with a confident assertion, "when you use Google services, you trust us with your information" and the first page states that "we've tried to keep this simple as possible". Essentially, Google uses ambiguous rhetoric and minimally adequate details and definitions so as to satisfy their advertising network while also attempting to minimize public discontent. While many people are critical of Google's lack of transparency, unveiling the inner workings of Google's 'black-box' would certainly spark public outcry that would profoundly outweigh the current discontent over transparency. Google defines personal information as "information which you provide to us which personally identifies you, such as your name, email… or other data which can be reasonably linked to such information by Google". The wording here is obscure, as Joseph Turow, researcher of 'digital cultural industries' suggests: does this mean that Google considers a detail to be personal information only if 'you provide it

to us'? If an advertiser provides the same information, will it not be considered 'personal' (2013, 178)?

Google collects comprehensive personal information from people using their services as well as exactly how people use their services. For example, a lot of personal information is logged by Google when you visit a site that uses Google's advertising services or when you view or click their ads and content. In other words, you do not have to click an ad on a website for Google to monitor you, you become monitored once you enter a site that uses one of Google's advertising services. In this way, Googles' data surveillance is rhizomatic as it is reflective of an untamed weed, it is tremendously expansive and regenerative (Haggerty and Ericson 2000, 614). Without substantial background knowledge regarding topics such as data mining and targeted advertising, many people could read the full policy and still not know that Google is processing information collected on and off of its services in an effort to construct social profiling categories that determine which ads, discounts, and news that is shown to you. This is troubling because "they help create the world they claim to merely 'show' us" (Pasquale 2015, 61).

2.2 Internet Privacy Laws and Regulations

The choice of analyzing Canada and the US is meaningful for a variety of political reasons. First, Canada scores near the top of the Economist 2020 democracy index in the category of "full democracies" while the US is near the top of the "flawed democracies" category. Second, Canada and the US are not just geographically near but up to 90% of Canadian internet traffic is regularly routed through the US (Deibert and Potter 2013), complicating issues of privacy and data sovereignty. Third, both countries have comparable internet usage at 93% of Canadians and

88% of Americans (World Bank 2021). Fourth, the divergent Overton window of each country suggests that historical or embedded socioeconomic structures significantly affect both individual policy preferences and policy outcomes. This begs the question: why is Canada's internet privacy laws much more in line with the EU than the US?

2.2.1 Canadian Laws and Regulations

In Canada, privacy regulations are unified among provinces under the federal government. The key legislation is the Personal Information Protection and Electronic Documents Act (PIPEDA) applies to the collection, use and disclosure of personal information in the course of a commercial activity. The Office of the Privacy Commissioner (OPC) to oversee compliance and monitor abidance to the federal privacy laws and regulations. PIPEDA defines personal information as "information about an identifiable individual". The OPC takes the position that "the information involved in online tracking and targeting for the purpose of serving behaviourally targeted advertising to individuals will generally constitute personal information". PIPEDA requires an individual's knowledge and consent for the collection, use, or disclosure of personal information. Express consent (opt-in) is required when dealing with 'sensitive information', whereas 'less sensitive' information can be dealt with through implied consent (opt-out). The 1983 Privacy Act predates the internet, but still outlines the rules for how the Canadian government is allowed to use the personal information of its citizens. Recently, Bill C-51 (the Anti-Terrorism Act) has been broadly criticized for reducing Canadian's privacy rights (especially online), by extending the power of government agencies to collect and share personal information. However, the provinces of British Columbia and Alberta also have their own

privacy legislations, the Privacy Information Protection Act (PIPA) which only apply to provincially regulated private sector organizations.

PIPEDA requires an individual's knowledge and consent for the collection, use, or disclosure of personal information. Express consent (opt-in) is required when dealing with 'sensitive information', whereas 'less sensitive' information can be dealt with through implied consent (opt-out). As for tracking children, PIPEDA requires 'meaningful consent'. While some information is inherently sensitive (e.g. medical records, religion), PIPEDA states that any information can be sensitive, depending on the context. Their example is that names and addresses of subscribers to a magazine would likely not be deemed sensitive unless it was "some special-interest magazine" (section 4.3.4). I suggest that what Google calls 'consent' to users for data collection "looks increasingly like monopoly and coercion" (Pasquale 2015, 81) as emerging start-ups are much more likely to sell their ideas to big companies because it is unforeseeable that they will be able to compete with giants such as Google.

Section 4 of PIPEDA contains rules that apply to every organization in respect to personal information. "Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified" (4.4.1); "Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent" (4.5). 4.4.1 is especially problematic because the business model of companies such as Google, Facebook, Amazon, etc. is to create accurate and comprehensive social profiles of its users in order to uncover how best to spark their buying impulses. In other words, since the purpose of Google's information collection is primarily to create behavioural profiles that are as

accurate as possible, Google cannot reasonably quantify how much personal information is necessary for their intended purpose. Moreover, "Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous" (4.5.3). Yet the 'information security' section of Googles' privacy policy has no mention of data retention policy.

2.2.2 US Laws and Regulations

In the US there is not a single unifying law regulating online privacy, instead a mishmash of federal and state laws applies. The US passed its Privacy Act 8 years before Canada in 1976, however, there is no similar body to the Canadian OPC to oversee compliance or a proper ombudsman check and balance. Instead, Americans must go to the courts with their complaints or charges. The Privacy Act is pre-internet and thus there are no such federal laws regarding online privacy similar to Canada or the EU. There The Federal Trade Commission Act (FTC) which regulates unfair or deceptive commercial practices and the Electronic Communications Privacy Act (ECPA) that protects certain electronic communications from unauthorized interception, access, use, and disclosure. Financial Services Modernization Act (GLBA) regulates the collection, use, and disclosure of personal information collected or held by financial institutions. However, the driver of privacy regulation in the US is based on corporate self-regulation.

In 2001 George W. Bush ratified the anti-terrorism statute called Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, known as the USA Patriot Act. The Patriot act is a complex and multifaceted legislation beyond the

scope of this research, the primary concern here is that the legislation broadens the electronic surveillance and wiretapping powers of federal law enforcement, and increases the information-sharing powers of investigative agencies; this was passed by both the House and the Senate, representing a shift in public and legislative thinking (Lyon et al. 2011). This legislation also affects Canada because it allows any digital information that passes through the USA to be collected, even if the information itself is not being stored in the US (Lyon et al 2014, 144); and as previously mentioned, 90% of Canadian internet traffic flows through the US.

2.3 The Operation and Context of Surveillance Capitalism

The field of digital studies is a highly interdisciplinary field drawing upon many corners of the social science and humanities canon(s). However, competing understandings of ICTs have entangled the discipline with a tension between analytical approaches. On the one hand, Jean-Francois Lyotard's *The Postmodern Condition* is dominant in understanding the digital condition where the digital transition creates a fundamentally new cultural and economic condition defined by a crisis of legitimacy and an "incredulity towards meta-narratives" (Wilkie 2011, 3); this focus on separation of knowing the particular from understanding the totality is typical of other digital studies scholars such as Donna Haraway, Mark Poster, and Michael Hardt. On the other hand, Rob Wilkie asserts that the digital condition of surveillance capitalism does not change the nature of social theories, since "Social theories are historical and an effect of the mode of production" (2011, 7). Theorists such as Shoshana Zuboff also take more of a marxist analysis focusing on a sort of capitalist accumulation characterized by increasingly invasive and extractive surveillance capitalism

The term *surveillance capitalism* was coined by Harvard social psychologist and philosopher Shoshanna Zuboff as an economic system that claims human experience as free raw material for translation into behavioral data. Although some of these data are used for product or service improvement, the remaining are declared as a proprietary behavioral surplus, fed into algorithmic processes called "machine intelligence," and constructed into prediction products that anticipate what you will do now, soon, and later (Zuboff 2019, 14). Neoliberalism is primarily blamed for the rise of surveillance capitalism. Specifically, the neoliberal vision of evading political ownership of deliberating difficult economic choices by placing an absolution authority on market forces "as the ultimate source of imperative control, displacing democratic contest and deliberation with an ideology of atomized individuals sentences to perpetual competition for scarce resources" (Zuboff 2016, 43). In other words, replacing the intermediary institutions of democracy such as regulatory boards, oversight commissioners, social safety nets, and unions with the solution of markets and competition as the ultimate truth of liberation.

2.4 Conclusion: Big Other

This neoliberal paradigm would diminish the checks and balances of market forces, mostly through supply-side reforms: including privatization, lower corporate and capital gains taxes, privatization, and deregulation. Zuboff highlights a meta-analysis of 1400 law review article from 1980 to 2005, their unanimous agreement was that industry regulation is a form of authoritarianism and so they unified around firm self-regulation with firms setting their terms, being able to monitor their own compliance and judge their conduct:

> By the time of Google's public offering in 2004, self-regulation was fully enshrined within government and across the business community as the most effective tool for regulation without coercion and the antidote to any inclination toward collectivism and the centralization of power (Orange 2019, 157).

While previous surveillance theories focus on state authority such as Big Brother, the greater worry today is what is known in critical digital studies as Big Other: entities manifest in the apparently friendly and harmless websites that know you intimately with hundreds of data points; Big Other: acts on behalf of an unprecedented assembly of commercial operations that must modify human behavior as a condition of commercial success (Zuboff 2019, 353). This complicates the dynamics of political research because now it is not simply the government with the ultimate authority but corporations and finance conglomerates that modify human behaviour and have highly focused efforts to drive and preserve an extreme free-market agenda at the expense of democratic values. These dynamics of corporate self-regulation (Big Other) then "replaces legitimate contract, the rule of law, politics, and social trust with a new form of sovereignty and its privately administered regime of reinforcements" (Zuboff 2019, 480).

Chapter 3: Epistemic Injustice and Democracy

3.1 Epistemic Injustice

3.1.1 Digital Testimonial Injustice

The problems concerning the power dynamics and unfair treatment in regards to communicative practices, where the comprehension and knowledge of individuals are involved, is known as epistemic injustice (Fricker 2007). Today, the use of cookies and black-box algorithms create 'filter bubbles' that cannot be viewed as ideologically or sociologically neutral nor should they be viewed as only improving the user's experience. Rather, these algorithmic processes can facilitate identity-based prejudices as a result of social categorization and behavioral prediction, partly by outsourcing our cognitive capacities and relying on algorithms that not even the software architects fully understand; this creates an act of epistemic injustice. One form of epistemic injustice is testimonial injustice, which occurs when an individual's testimony is not taken seriously or is considered unreliable because of prejudices and stereotypes regarding their identity; the systematical prejudices, premised on economics position, race, social class, religion, sex, etc., establish the typical forms of testimonial injustice (Scotto 2020, 157). For example, the police not believing in an African-American's story because of his race and/or social class. If 'filter bubbles' are drivers of echo chambers or facilitate polarized content based on one's 'suspected' views and interests, this leads to a reinforcement of negative stereotypes that influence people's offline behaviour, including voting.

3.1.2 Polarization and Power Asymmetry

Polarization is not necessarily a form of epistemic injustice in itself, and polarization does not have to involve epistemic injustice to be problematic. However, the algorithmic facilitation of

polarization serves to reinforce several forms of testimonial and hermeneutic injustice. This begins by placing users at a severely disadvantaged position epistemically in comparison to the power and capacity for control held by datafication and dataveillance systems. For example, Facebook's input of users behaviour data combined with the platform's social ranking and output of news information generates a new form of informational power that results in a structural power asymmetry that is unable to be seen by users. Facebook is the primary source of news in most countries, typically holding roughly thirty-five percent of the market (Fletcher 2020). A user's news feed is created based on their online behaviour of clicks and past likes, including sensitive data such as which news headlines you 'like' or which organizations you interact with. The news feed then facilitates news (or other political content) that is similar to the database's perceived views of the user and scarcely will Facebook reveal political content that opposes such views. Kitchens et al 2020 demonstrate this by analyzing two-hundred-thousand Facebook users over four years. They find that the more time an individual uses Facebook, the more polarized their news consumption becomes; and that Facebook usage is five times more polarizing for conservatives than liberals. Hence, the algorithmic mechanisms are largely invisible yet they have potent implications for obscuring one's social experience. If habitual use of social media does exacerbate epistemic cleavages, can such datafication be said to be enhancing or diminishing human capacity or agency? What is clear though is that user's cognitive outsourcing to databases can no longer be characterized in a neutral or innocent fashion.

3.1.3 Digital Hermeneutic Injustice

Hermeneutic injustice is "the injustice of having some significant area of one's social experience obscured from collective understanding owing to a structural identity prejudice in the collective

hermeneutical resource" (Fricker 2007, 11). In other words, this injustice occurs while individuals or groups are not fully aware because of the cultural context in which they are marginalized, and so they fail to recognize and denounce the injustice (Piras 2021, 35). Thus, the increasing polarization of user's 'news diet' facilitates an epistemic cleavage between liberal and conservative worldviews resulting in a hermeneutic injustice where credibility becomes increasingly entangled with ideology. However, this injustice is not just about digital literacy or media literacy, because the 'black-box 'algorithms used on social media, by definition, are not publicly accessible to see, only the inputs and outputs of the databases can be seen. Without transparency, all data operations in the back-end of social media will rarely be reasonably mechanical or function in an explicit fashion.

> All types of treatment that disturbs, conditions, manipulates, weakens or ignores people's capacities in virtue of the conditions in which the communicative interactions are produced, involving knowledge and information, meanings and interpretations, is covered by the concept of epistemic injustice. (Scotto 2020, 157)

The epistemic injustice regarding agency and identity is not just for isolated individuals, but between the intersections of individuals and their epistemic communities who are separated in various ways. This is highlighted by the concept of the digital divide, referring to "the gap that separates people from groups, in virtue of the generation, regional, socio-economic, and 'cultural capital' distance" (Scotto 2020, 156). An analysis of the intersectionality of these demographic variables (inputs) accompanied by datafication and dataveillance (operation), and social media feeds (outputs) can help us explain the similarities and disparities of user experience online. These intersectionalities provide focal points to where patterns of epistemic injustice can be found structurally on social media.

3.1.4 Systematic Epistemic Injustice

Surveillance capitalism displays this injustice systematically as a situated hermeneutical inequality by social profiling and manipulating the information that will be central to the users eyes and the information that become scarce or invisible. It is daunting how advertisements and discounts online have begun to alert people of their social position (Turow 2015, 6). 'Lower-class' people are realizing that their online ads are consistently for cheap cars, regional vacations, and fast food discounts for example. This is troubling because such people will have a narrow view of the world's opportunities in comparison to someone who is regularly shown ads for national or international trips and luxury products (Turow 2015, 6). Essentially, individual social profiles are turning into evaluations of your reputation for market desirability. The majority of users are likely unaware that online stores often charge users different prices at the same time of day depending on their behavioural data. In addition, a company such as Expedia or Trivago that promises a 'price guarantee' in the US is not legally required to always display the cheapest price they have. Turow was correct when he suggested that people will eventually realize how such advertising segregates them and pits them against others in the ads and discounts they receive (or the targeted news stories). Subsequently, people will begin to suffer the consequences of discrimination.

Google often determines what possibilities reach our awareness, their online search and advertisement monopoly is beginning to profoundly influence our decisions regarding what we do, think, and buy (Pasquale 2015, 59). Pasquale discusses how such new media giants are losing trust because users cannot tell if results (or ads, or news) are based on statistical prominence or through personalization algorithms; even if just statistics are used, what kind of statistics? Google does not make their database algorithms public. Pasquale is clearly correct in his

assertion that “the power to include, exclude, and rank is the power to ensure which public impressions become permanent” (2015, 61). While we pay no money for Googless services, we are certainly paying with our data and ignorance; extensive and valuable information is collected as Google processes billions of search queries each day (not to mention data collection of its other services). As Googles’ advertising network has risen to monopolistic proportions, it has become difficult to know whether your top search results “reflect(s) its quality or its willingness to pay for visibility” (Pasquale 2015, 70). That being said, it is troubling that Googles’ advertising network often exploits the assumption that commercial messages that pose as soft news or entertainment are more persuasive than traditional straightforward ads (Turow 2015, 6). Is it undoubtedly unethical for Google to mix paid content with supposedly neutral entertainment or news content. Therefore, such an activity is in fact manipulating all individuals of society since Googles’ assertion of neutrality is dubious when the business model is based on behavioural datafication and consequent manipulation.

3.2 Informational Power

The driving force of digital epistemic injustice being intrinsic to surveillance capitalism is a new form of informational power, namely, ‘instrumentarianism’; coined by Zuboff (2016, 331) as “the instrumentation and instrumentalization of behaviour for the purposes of modification, prediction, monetization, and control”. Thus, this can operate as both explicit prejudicial power and discreet prejudicial power at the structural level where datafication processes are specifically designed to be unknowable by users. In the critical digital studies literature, ‘instrumentation’ generally refers to the omnipresence and interconnectedness of datafication networks that capture, decipher, and actuate human experiences; while ‘instrumentalization’ refers to the social

relations that familiarize social media companies (and companies on the behavioural-futures market) to human experience as a form of surveillance capital. Said plainly, this informational power refers to the dedication of surveillance capitalists to transform users into atomized means for market forces. The epistemic cleavage between social media datafication and users then constitutes a social inequality where human agency and the self-determination of identity are eroded. This is a kind of hermeneutic injustice because it concerns the conceptual repertoire of epistemic groups and substantially weakens the intelligibility of user's very own expressions as subjects of social understanding (Fricker 2017); similarly, it curtails the ability to provide or receive knowledge as autonomous agents. Overall, the behavioural data capture and mass outsourcing of cognition to black-box datafication generates critical confusions and disorientations of power, authority, and epistemology.

If our digitally mediated society is aiming for transparency and fairness then "we need to understand the industrial forces that are defining our identities, our worth, and the media environments we inhabit" (Turow 2015, 9). Googles' black-box system is reflective of Jeremy Benthams' panoptic central guard tower; Google administrators can extensively track users' behaviour while users are largely unaware as to when and how they are being precisely monitored. Each social profiling category has a panoptic effect, which are often unique from each other; then, since Google has monopolistic control over the prominence of information, they are able to influence and modify users' behaviour in a panoptic fashion. This illustrates how people on the internet do not exist as autonomous individuals, but rather as a product of social media databases (and behavioural futures markets) that monopolize behavioural data to continually alter users' decision making, and therefore their agency and identity.

3.3 Democracy Implications

Changing identities and agency in the digital condition is significant because sites of sovereignty become entangled with digitized identities and experiences of false free will. This worry of individual powerlessness leads to a dilemma of hermeneutic injustice where "the powerful have an unfair advantage in structuring collective social understandings" (Fricker 2007, 2) which leads to developmental and cognitive disadvantages. In democratic theory, for people to function well civically, there must be a network of intermediary institutions (such as unions, parties, news, media, etc.) that enable individuals to get information and inform judgement. However, the current literature suggests that the internet breaks down these institutions and creates a fragmentalization of ideologies. Information environments have significant ramifications for identity and democratic citizenship. Democratic theory assumes that voters have a reasonably shared understanding of what is happening, in other words, a common political world. What happens to democracy when citizens lack a reasonably common understanding? Digital footprints used to categorize, predict and manipulate users' actions, typically establish 'filter bubbles' keeping the ones that think alike us near, and far from those who think differently, segregating and marginalizing epistemic communities. Thus, algorithms of datafication decide or 'pre-personalize' which information should be invisible to you, and which should be central to your viewing. In this way the data processes can begin to alter user behaviour and their ability to recognize or interpret how and why certain content is central to their digital experience. Therefore, sites of offline autonomy can become entangled with digitized identities and experiences impeding free will.

With the pervasiveness of the internet today, algorithms become a new form of power facilitating the shift from enclosed structures to entangled systems. This is best exemplified by the paradox of freedom and control for users on the internet. On the one hand, users have virtually unlimited access to media, knowledge, and information. On the other, behaviour data is constantly mined while users are no longer geographically tied to places of work or sites of consumption. To the extent that individuals have control over their interaction with others forms a key pillar of one's identity, users do not have a digital identity except for what datafication occurs within private social databases (Ray 2021). Thus, the power of algorithms and datafication represents a new normative problem arising for democracy, namely, the ability for users to understand datafication capabilities and their effects on them as political agents.

3.4 Conclusion

The issue of digital epistemic injustice is not that internet networks can increase or outsource our cognitive capacities, rather, it is that datafication operations are created to "usurp our authority as experts in view that we overestimate their capacity to understand what they do beyond their competence" (Scotto 2020, 174). In all, the separation of users from their data reduces the capacity of us to assert control over the nature of one's agency, a key tenet of both humanness and democracy. Overall, the informational power asymmetry between users and social media platforms is the root cause of this epistemic cleavage, a credibility crisis.

Chapter 4: Social Media and Political Attitudes: Who Shapes Who?

While it is clear that social media algorithms such as filter bubbles do alter user behaviour, it is more difficult to establish whether such social media tools are the primary driver of political polarization we see today. The intimate dynamic between political attitudes and social media poses an arduous challenge for social scientists, since it is infamously difficult to uncover whether political attitudes shape social media, or vice versa (Bail et al. 2018, 9216). As previously mentioned, Kitchens et al.'s study exemplified the power of Facebook news feeds in terms of driving liberals more left and conservatives (significantly) more right. However, this finding is standard among the literature of group polarization studied in *offline* environments. When like-minded people group together, their group attitudes become more extreme than the median attitudes of the group's individuals. Sunstein (2009, 8) illustrates how this is even seen among US federal judges, when panels are composed of only one party, like-minded judges will go to extremes; thus, those who are supposed to be specialists are no less likely than regular individuals to be pushed to extremes.

4.1 Information Exposure and Partisanship

As the Covid-19 crisis worsens as countries enter their third and fourth waves, it may seem intuitive that rising global case counts and new mutations may reduce vaccine hesitancy. However, there is a stark group rift between liberal and conservative voters in terms of both vaccine efficacy, trustworthiness of public health officials, and perceptions of Covid-19 threat levels. In the U.S. Republican voters have shown a declining favorability and intention towards receiving Covid-19 vaccines since the beginning of the pandemic while Democrat favorability and intention have remained largely stable (Fridman 2021). Thus, some groups are indifferent to

public health issues that markedly worry others. Fridman (2021) suggests that differing exposure to news channels and social media could explain this asymmetric polarization. This resulting group polarization is virtually analogous to issues such as climate change. The driving force for such asymmetric polarization is differing information exposure, in other words, an epistemic cleavage. If a group is exposed to information that demonstrates how climate change poses severe consequences, and if the view becomes commonplace in an epistemic community, it is likely that pertaining individuals may end up fearful. In contrast, if one's epistemic community encounters very little information concerning climate change risks, except that opposition voters are fearful, one is more likely to ridicule such fear (Sunstein 2009, 23).

A key driver of group polarization derives from the way 'filter bubbles' become a catalyst for intragroup corroboration and inhibitors of intergroup deliberation. This results in lowered attitudinal diversity within groups and greater epistemic rifts between groups. For example, an individual who is unsure what to think about an issue and lacks confidence in their predisposition is more likely to moderate their view; however, if others appear to hold a similar predisposition, the individual will become considerably more confident that their opinion is factual (Sunstein 2009, 23). While this process of increased confidence usually occurs for all group members- which is difficult for an individual to recognize- it becomes exceedingly more difficult to recognize over social media. This is because of the added layer of black-box algorithms to the dynamics of group psychology: not only do individuals know very little about how their online experience is pre-personalized (personalized remotely from their behavioural data), they will necessarily know even less about how other user experiences are pre-personalized. For example, it is difficult to ascertain whether a group member's climate change denial is purely their view

without hesitation; or whether their attitude is derived from social media amplifying and polarizing their initial predispositions.

4.2 Reputation and the Characteristics of Group Affiliation

Of course, individuals want to see themselves in a positive light and also to be perceived positively by their group counterparts both offline and online. In Bail et. al's (2018) experiment, Democrat and Republican twitter users were made to engage in a twitter bot of an ideologically opposed thought leader or organization, after one month Democrat attitudes remained stable while Republican attitudes became substantially more conservative. Were Republic ideological shifts a reaction to the messages (i.e. information exposure) or to the messengers? While more studies are needed to solidify a robust conclusion, it is clear that group membership is often more important than the political issues at hand. Such asymmetric polarization is at least partly the result of identity-based prejudices; these emerge alongside intragroup reputation development and constitute a form of testimonial injustice. While increasingly polarized information exposure and intergroup corroboration begins the vicious cycle of group polarization, what largely expedites this cycle is social media's role in reputation development.

Online reputation (or identity) development can take place over the passive reading and brief engagement with news feeds or via more comprehensive engagement with discussion forums or blogs. In either medium, the role of social comparison appears to be heightened and more complex than in offline deliberation venues. In a 2016 Pew Research survey, the vast majority of individuals view social media as a place where individuals are afraid to present their opinions for fear of criticism or the loss of friends; and regard social media as a venue where users regularly

overstep the boundaries of face-to-face discussion. In other words, this suggests that social media either directly or indirectly incentivizes reactionism as opposed to civil deliberation, a key characteristic of what scholars call post-truth politics. This can be seen in the way 2016 election candidates' Tweets are substantially more likely to be re-Tweeted when they are explicitly emotive and describe moral outrage (Bradey et al.2018). The prominence of news and advertisements intent on reactionism is especially troubling in the era of "fake news". That is to say, it is not simply that facts are threatened but they are becoming less relevant to political discourse and media engagement.

4.3 Post-Truth Politics and Social Media Amplification

In 2016 Oxford dictionary deemed *post-truth* as the word of the year and added it to their dictionary editions the following year. *Post-truth* is defined as "relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief" (Martin 2016). As has been noted, social media platforms bolster filter-bubbles and echo-chambers. This incentivizes confirmation bias particularly when the goal of a news story or political advertisement is not truth but shareability. For this reason, the rise of clickbait from fake news bots has been incredibly powerful and substantially irrepressible. Bovet et Makse (2019) uncovered that in the five months preceding the 2016 US election, roughly 25% of tweets containing links to news outlets were either fake or extremely biased news (Gugleilmi 2019). Today, social media's overtaking of traditional news platforms has been rapid and far-reaching, individuals' primary exposure to politics and news is undoubtedly from their social media feeds. However, Facebook and Twitter assert that they are technology corporations run fundamentally by algorithms, and not media companies with journalistic responsibility. While

fact-checking pilot programs have now begun on Facebook and Twitter, recent data suggests that fake social media accounts are harder than ever to detect (Ferrera 2020).

4.4 Case Study: Environmentalism, Social Media, and Epistemic Injustice

Over the last two decades climate change has become among the most important political issues as well as the most polarizing. As a result of rapid fossil fuel expansion since the industrial revolution, the biosphere has now begun to transition away from the Holocene- the geological epoch responsible for providing stable atmospheric conditions for humanity to prosper. Humanity is now entering a proposed new epoch called the 'Anthropocene', as a result of substantial anthropogenic changes to the functioning and structure of the biosphere, including the climate system (IPCC 2018). Today, there is scientific consensus that climate change is human-driven, moving at a rapid pace, and destined to cause significant adversities for humanity. However, if one is to follow primarily (or solely) conservative news sources in North America, then it will seem as though the science is very unclear and inconclusive. Scientific consensus is not about unanimity among scientists, but rather a collective judgement reached by institutions derived from a supermajority of individual judgements by scientists. Furthermore, a paradox arises in the US where those opposed to regulating pollution are among the most hurt by pollution, Republican states (Hochschild 2016, 9). If the science is clear, why is climate denialism and anti-environmentalism so prevalent among Conservative voters? If there is a societal trust of scientists for developing computers, cars, rocket ships, medical equipment, etc.; why does this social trust stop at climatology (and until recently, epidemiology)?

Psychological studies suggest that acceptance of conspiracy theories, including the 'hoax' of climate change, creates 'self-defeating' outcomes such as suppressing a readiness to act and feelings of autonomy (Douglas et al. 2017). As a result, these individuals feel a sense of disenfranchisement and helplessness. Research suggests that:

> people may be drawn to conspiracy theories when — compared with nonconspiracy explanations — they promise to satisfy important social psychological motives that can be characterised as epistemic (the desire for understanding, accuracy, and subjective certainty), existential (the desire for control and security), and social (the desire to maintain a positive image of the self or group).(Douglas et al. 2017, 538)

With this in mind, it is now social media that plays the most significant role in provoking these psychological tendencies by relying on filter-bubbles, generating social exclusion, prioritizing post shareability over truthfulness and transparency, and increasingly exposing users to disinformation and extremely conspiratorial content.

There are several epistemic motives that tend to bolster beliefs in conspiracy theories or fake news (including grossly biased news). For example, climate change: when events are particularly significant or large in scale and render individuals discontented with mundane, parsimonious explanations (Douglas et al 2017, 539). Recent research suggests that those identifying as Conservative tend to share the most fake news, however, there are liberals (and leftists) who also share fake news; the most interesting finding is that the most fake news is shared at the fringes, those near the edges of the political spectrum (Hopp et al., 2020). Thus, if social media substantially exacerbates polarization as the current literature suggests, then the epistemic cleavage within scientific, yet partisan issues, becomes inflamed by regular social media use. That is to say, as more users are pushed to political fringes, fake news becomes more widely shared and believed in. Conspiracy theories and alternative facts seem to supply "internally

consistent explanations that allow people to preserve beliefs in the face of uncertainty and contradiction" (Douglas et al. 2017, 539). As polarization is heightened online, users are more able to easily satisfy these social psychological motives since persuasive fake news is able to provide such cognitive closure. A hermeneutic injustice is generated where users are then less able to understand themselves nor a common political reality with those users on the other side of the political spectrum.

Social media plays a critical role in climate change denialism by fragmenting the traditional network of intermediary institutions which enable people to inform their judgements. The current literature suggests that the majority of internet users have a dismaying ability to identify fake news (Nightingale et al. 2017). Beyond fake news (including grossly biased news and misreporting), most users have difficulty differentiating between "sponsored content" articles and real news stories (Wineburg et al. 2016). This hindrance to informed judgement constitutes several forms of testimonial injustice. In the same way that like-minded groups have a more extreme attitude than the median attitude of each individual, pre-personalized social media feeds tend to be more partisan than the user's actual political attitudes. This is an underlying force found in the asymmetrical polarization of conservative internet users, whose robust loyalties to increasingly far-right wing news sources partly relies on the intragroup demonization of centrist and liberal news sources. With a lack of social media referees and the algorithmic prioritization of shareability over legitimate information, prejudice and indiscretion curtail the civil deliberation that may have been dreamed of for the internet decades ago.

4.5 Informational Power and Democracy: The Epistemic Linkage

When individuals (a) do not have control over their personal data, (b) misinformation and disinformation is easily spread online, and (c) advertising (whether political or commercial) lacks transparency and user understanding, then a credibility crisis emerges. The most significant issue with fake news dissemination online is not that people will believe in misinformation or grossly biased news; although that is an issue. The greatest issue is that genuinely credible information sources become perceived as discredited or illegitimate by large demographics of users. The best example of this phenomena is exemplified by the Donald Trump administration's attack on 'fake news' and support for 'alternative facts'; with the support of corporate interlock from conservative media giants such as FOX news. Over Trump's 2016 election and his following administration, he has alleged at least twenty-four conspiracy theories (Bump 2019), the first president to make conspiracy theories an integral part of a platform or administration. The goal of this fake news campaign is not primarily to make voters believe in these conspiracies. The goal is to generate doubt for the intermediary democratic institutions (news outlets, unions, parties, popular media, etc.) where voters can traditionally obtain informed judgement. In other words, the goal was for voters to distrust all sources of information, even credible sources; therefore weaponizing an epistemic cleavage of testimonial injustice. When citizens distrust credible news sources in mass, this paves the way to make the government less accountable, therefore rendering individuals powerless to market forces.

This weaponization of disinformation and epistemic cleavages is not unique to political campaigns, rather, it is emblematic of the epistemic links of surveillance capitalism and the power asymmetries between users and social media platforms. This favorability towards market

forces and self-regulation was not only attractive to policy makers because of reducing accountability for difficult policy choices, but also because this neoliberal vision promised to:

> Impose a new kind of order where disorder was feared. The absolute authority of market forces would be enshrined as the ultimate source of imperative control, displacing democratic contest and deliberation with an ideology of atomized individuals sentenced to perpetual competition for scarce resources. (Zuboff 2016, 43)

Comparatively, the algorithmic weaponization of information via the datafication of behavioural information is necessarily outside of the users' sight and knowledge. In other words, the interpretive resources available to internet users are necessarily 'cognitively diminished' as a result of algorithmic social categorization; the power of dataveillance to aggregate personality, emotional, and demographic data points in order to predict and alter the behaviour of people as members of epistemic groups shows that black-bock dataveillance is prejudicial by design and can often constitute a hermeneutic injustice in and of itself. One way social media is prejudicial by design is that the dataveillance operation facilitates mass indirect discrimination, which is: an arrangement, rule, or practice that "applies in the same way for everybody but disadvantages a group of people who share a protected characteristic, and you are disadvantaged as part of this group" (EqualityHumanRights 2021). But even if these algorithmic prejudices and resultant discriminations may not be intentional or explicitly deliberate, this does not render datafication as epistemically neutral nor should it produce a deficit of corporate social responsibility.

4.6 Conclusion

To clarify, fake news, misinformation, and disinformation are examples of *explicit* datafication prejudices, however, there is an underlying issue of concealed and superimposed prejudice that is *implicitly invisible*. Since social media datafication is not widely understood, even by the creators of such operations, it is a 'black-box science': "It is now possible to make – very

indirectly – things that do what we want them to do but which we really cannot understand" (Dennett 2020, 39). The black-box nature of social media's institutional design means that the datafication (or dataveillance) is conducted on a layer that is not accessible to any user. The more covert level of digital epistemic injustice occurs "in virtue of the logic and the design that rules its functioning, and, therefore, operating without the knowledge, consent, or control of the users, they can cause even deeper epistemic damages" (Scotto 2020, 162). That is to say, it is not the digital interactions of users that is most important necessarily, but the predictive signals that news organizations, political marketers or companies can extract from such interactions. Thus, the problem is not social media per se, but the institutional design of datafication that does not recognize social media as inherently a political sphere. Under one form of technology i.e. social media datafication, institutional design can either become emancipating or dehumanizing. This obscurification of users' social experience relies upon a structural identity prejudice, namely, the algorithmic profiling, categorizing, and predicting mining within databases, constituting a hermeneutic injustice. Without datafication transparency alongside the neglect to show users how their own behavioural data affects them, users' socio-political self-understanding will continually be artificially compromised. With this in mind, social media datafication becomes an issue beyond just privacy, it becomes an issue of social justice and epistemic inequity.

Chapter 5: Discussion

5.1 The Scientific Pedestal and Techno-determinism

The utopian visions for the internet included the democratization of information, the empowerment of disenfranchised voices, and thus, the augmentation of human agency and autonomy. However, it is clear that technological advancement left unchecked can easily diminish the democratic capacity and accountability of individuals and groups. In order to understand the ethics and politics of data science, or specifically *dataveillance*, one must first understand how 'science' is first and foremost a social institution. In the twentieth century it was evident that 'science' has replaced religion as the dominant form of social legitimation (Lewontin 1991, 1-2). As a result, 'natural science' has been regularly insulated from the social sciences and humanities in quite an invalid fashion. Science has been placed on a pedestal, treated as an objective, nonpolitical, true for all time body of knowledge that transcends all other ways of knowing and all other endeavors (Lewontin 1991, 8). Today, this pedestal positionality is at the same time a cause and consequence of how social media data science has become the ultimate 'black box'. To reiterate, a 'black box' is "anything having a complex function that can be observed but whose inner workings are mysterious or unknown" (Collins Dictionary 2021). The 'natural sciences' have been extensively emancipatory throughout much of history, which has led to its social legitimation, even when the inner workings of the discipline are mysterious or unknown to most of society at large. But the misguided vision of 'science' as inherently neutral or innocent has undermined the power of other academic lenses to be valid avenues of inquiry.

One should not need to be a certified data scientist or computer scientist to understand what is at stake with the status quo of surveillance capitalism. In other words, the 'black box' of data science ought not to be left to the 'experts' per se, but rather, such data science should be transparent and cognitively accessible to the layman. The concern is not in the nature of outsourcing (or increasing) cognitive capacities to intelligent machines, the concern is for particular structures of "intelligent designs that will usurp our authority as experts in view that we overestimate their capacity to understand what they do beyond their competence" (Dennett 2020, 400). Thus, the operation of social categorization for the purpose of pre-personalizing digital experiences leads users down divergent paths of political realities where the capacity for individuals to interpret a common political world becomes curtailed. This solidifies the linkage of digital epistemic injustice to an era of democratic deficit(s). A neglect to address these datafication designs then leads to a devaluing of human agency, autonomy, and self-determination, the foundational pillars of democracy.

Modern science has arguably been the greatest institution for the betterment of humankind thus far, however, it is important to understand that "biology is a discourse, not a living world in itself" (Haraway, p.298). In the world of social media, data science is not inescapably 'objective', it is a situated knowledge. On the extreme end, "Science is in any day what scientists do and defend. [20th century] Eugenics fell squarely in the mainstream of scientific and popular culture" (Kevles, p.326). Today, dataveillance is a part of nearly all aspects of society from video games, medicine, employment, and urban planning, not just social media. We rely on modern science's remarkable capacity of datafication for what is taken for granted as 'normal' daily affairs. This all-encompassing reliance on science results in scientific inquiry and application to

be largely informed by social, economic, and political forces. This can be problematic because "those forces have the power to appropriate from science ideas that are particularly suited to the maintenance of and continued prosperity of the social structures which they are a part" (Lewontin 1991, 1). With this in mind, we can see how the influence of social media platforms over individual (and group) identity and agency is not techno-deterministic. Instead, the status quo of surveillance capitalism fits neatly within modern historical developments, namely, the convergence of the neoliberal zeitgeist with all facets of emerging technology. In all, the epistemic conflicts of surveillance capitalism are primarily a dilemma of *capitalistic tendencies* rather than a dilemma of *surveillance*.

5.2 A Path Forward

An exhaustive account of possible solutions to the woes of epistemic injustice within surveillance capitalism is beyond the scope of this paper; however, it is fitting to briefly elaborate on such perspectives in the literature which show promise. The solutions to Surveillance Capitalism's effect on human agency and democracy can only be partly found in themes of technological regulation and media literacy; this will prove to be a Band-Aid in a wound requiring structural rehabilitation. This is because the operation of dataveillance is not entirely determined by particular Big Data actors, the logic of social media entails a new political economy of information that compels platforms to disorientate informational power and authority. The facilitation of asymmetric polarization on such platforms is the earmark example of how the design of Big Data can usurp any authority of experts, therefore, establishing a credibility crisis. The effect of filter bubbles is not just polarization, but the ability to generate a digital ecosystem of feedback loops that segregate ideologies into increasingly insulated

epistemic communities. The digital markers of online behaviour that is captured and translated into a predictability and manipulatory commodification occurs not just without user's consent (typically), but without even the user's knowledge; this is the key distinction that makes surveillance capitalism *surveillant.* Thus, the centralization of surveillance capital by social media requires the expropriation of users' data as a necessity of its market logic.

This 21st century political economy of capturing behaviour data as a raw material to be commodified converges with the development of Moral Limits of Markets (MLM) theories. While some markets may nurture freedom, others may curtail freedom substantially. Libertarians and neoclassical economists view markets as 'homogenous institutions', MLM theorists such as Debra Satz or Michael Sandel reject this assumption and assert that the particular individual and societal effects of each market ought to be critically examined. General egalitarians recognize that markets can reflect systemic inequalities, however, they see the solution as *ex-post* e.g. taxations and redistributions in a labour market; Whereas particular egalitarians would prefer to restrict those markets *ex-ante* where systemic inequalities unfold (Satz 2010, 68-70). In terms of surveillance capitalism, an ex-ante solution would be to resecure users control over their data, enforce datafication transparency, and combat the algorithmic designs which catalyze the shareability of misinformation. In fact, these measures are supported by the creator of the internet himself, Tim Berners-Lee, who is now developing 'Solid'- an open-source project to reclaim personal data as well as restore the power and agency of individuals on the internet (Inrupt 2018).

The power of surveillance capitalists means that this decentralization project is not an easy objective by any merit. But if successful, this project could essentially decentralize the internet and substantially curtail the effect of social media's machine intelligence. Thus, the burden necessity here is to address the *platform monopolies* held online. Berners-Lee heads the Web Foundation, a lobby organization on a mission to ensure digital equality through policy change. But this foundation is entangled in a corporate interlock because of its reliance on Google and Facebook donations. That is to say, will technology platforms purposely lobby to regulate their datafication designs, increase transparency, and reject the commodification of human experience? Thus far, this has not been the case. However, it seems that working with big tech is the inevitable path forward. "It has taken all of us to build the web we have, and now it is up to all of us to build the web we want" (Berners-Lee 2017).

Conclusion

Overall, sweeping engagement with the internet has the ability to significantly alter identity and agency; left unchecked, these common datafication processes can establish or help reinforce avenues of hermeneutic and testimonial injustice. Surveillance capitalism facilitates this injustice systematically as a situated hermeneutical inequality by commodifying human experience (inputs); social profiling, predicting, and manipulating an individual's future behaviour (operation); and determining what information will become central to the users' eyes and what information will become scarce or invisible (outputs). These epistemic injustices (which become outputs and eventually feedback into inputs) emerge by placing users at a severely disadvantaged position epistemically relative to the power and capacity for control held by datafication and dataveillance systems. This extraction and expropriation of personal data illustrates how individuals on the Web do not exist as autonomous individuals, but rather as a substantially atomized product of social media dataveillance. With the omnipresence of datafication today, algorithms have become a new form of power facilitating the shift from enclosed structures to entangled systems of knowledge, power, and authority. This reconditioned form of agency in the *digital condition* is troubling because sites of personal sovereignty and offline autonomy become entangled with digitized identities and experiences of false free will online.

The individual and societal effects of these outputs (i.e. epistemic cleavages) is currently best exemplified by the nature of political polarization in the digital media ecosystem. Polarization is not inherently a form of epistemic injustice in itself, and polarization does not need to concern epistemic injustice to be problematic. Nonetheless, the algorithmic abatement of polarization serves to reinforce several forms of testimonial and hermeneutic injustice. When like-minded individuals are grouped together the overarching views of the epistemic group routinely becomes

more extreme than the median attitude of its members. But online, this dynamic of group membership artificially intensifies both explicit and covert prejudices that push users into insulated epistemic realities, facilitating a primacy on partisanship over knowledge credibility. Overt epistemic injustice can be found in the analyses of algorithmic abatement of fake news, disinformation, and grossly biased news. However, the more innocuous element of digital epistemic injustice is *covert* because dataveillance operations are designed to alter human behaviour while being operationally unknowable. This constitutes a hermeneutic injustice because it concerns the conceptual repertoire of epistemic groups and substantially weakens the intelligibility of user's very own expressions as subjects of social understanding. Furthermore, this diminishes the capacity of users to provide or receive knowledge as autonomous agents. Accordingly, the behavioural data capture and mass outsourcing of cognition to black-box dataveillance generates critical confusions and disorientations of power, authority, and epistemology.

These entanglements of informational power pose a serious threat to democratic backsliding by disrupting the key pillars of democracy at individual and epistemic group level of analysis. First, democratic theory assumes that voters have a reasonably shared understanding of what is happening i.e. a shared understanding of underlying facts- a *common political world*. Today, a hermeneutic injustice has been perpetuated by dataveillance where users have a diminished capacity to understand themselves nor a common political reality; especially with those users on the other side of the political spectrum. Second, democratic theory recognizes that for individuals to function well civically, there must be a network of intermediary institutions (e.g. unions, parties, news, media, etc.) that enable individuals to get credible information and inform their

judgement. The intelligent design of social media datafication breaks down the credibility of these institutions, resulting in a fragmentalization of knowledge, power, and authority. This ensuing credibility crisis is a form of testimonial injustice, best exemplified by the asymmetrical polarization of conservative news sources, where the pulling of individuals towards the ends of the political spectrum results in a segregation and insulation of perceived epistemic credibility of information and knowledge sources. These resulting digital epistemic cleavages are also significant because they create a gap between what users know about themselves and what social media platforms know about them, hence facilitating the epistemic powerlessness of individuals. This raises the normative dilemma of accountability, because if voters feel powerless then their capacity to hold the government accountable is desperately curtailed.

Finally, there remains significant hope for the future of digital epistemic justice, but scholars ought to recognize that this epoch of surveillance capitalism is more of an issue of capitalistic tendencies than an issue of surveillance itself. That is to say, this epoch fits neatly into the historical development of neoliberal capitalism, a market logic that seeks to commodify new spaces, representing the dematerialisation and deterritorialization of capitalistic frontiers. Thus, technological determinism should be avoided because the solutions will be found with regulatory policy and law. This is not a demonization of Big Data per se, but this is a rejection of the societal normalization of current dataveillance designs. To preserve democracy, the emergent societal perspective (of techno-determinism) that believes data expropriation and dataveillance is normal or inevitable must be rejected. Further inquiry is required concerning the moral limits of markets and what realms ought to be surveilled in the first place. “Society develops a type of

self-censorship, with the knowledge that surveillance exists - a self-censorship that is even expressed when people communicate with each other privately" (Assange 2017).

References

Bail, Christopher A., Lisa P. Argyle, Taylor W. Brown, John P. Bumpus, Haohan Chen, M. B. Fallin Hunzaker, Jaemin Lee, Marcus Mann, Friedolin Merhout, and Alexander Volfovsky. 2018. "Exposure to Opposing Views on Social Media Can Increase Political Polarization." Proceedings of the National Academy of Sciences 115 (37): 9216–21. https://doi.org/10.1073/pnas.1804840115.

Bump, Philip. n.d. "Analysis | President Trump Loves Conspiracy Theories. Has He Ever Been Right?" Washington Post. Accessed September 30, 2021. https://www.washingtonpost.com/politics/2019/11/26/president-trump-loves-conspiracy-theories-has-he-ever-been-right/.

Balkan, Aral. "We Didn't Lose Control – It Was Stolen." n.d. Accessed September 30, 2021. https://ar.al/notes/we-didnt-lose-control-it-was-stolen/.

Berners-Lee, Tim. 2018. "One Small Step for the Web…." October 22, 2018. https://inrupt.com/one-small-step-for-the-web.

Boxell, Levi, Matthew Gentzkow, and Jesse Shapiro. 2017. "Is the Internet Causing Political Polarization? Evidence from Demographics." w23258. Cambridge, MA: National Bureau of Economic Research. https://doi.org/10.3386/w23258.

Brady, William J., Jay J. Van Bavel, John Jost, and Julian Wills. 2018. "An Ideological Asymmetry in the Diffusion of Moralized Content among Political Elites."

"Consolidated federal laws of Canada, Personal Information Protection and Electronic Documents Act." Legislative Services Branch. March 23, 2017. http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html#h-5.

Deibert Ronald, and Mitch Potter. "Canadians Not Safe from U.S. Online Surveillance, Expert Says." Thestar.com. June 08, 2013. https://www.thestar.com/news/world/2013/06/07/canadians_not_safe_from_us_online_surveillance_expert_says.html.

Dennet, Daniel C. 2020. "The Age of Post-Intelligent Design". In *The Age of Artificial Intelligence: An Exploration*, edited by Steven S. Gouveia, 27-63.Vernon Press Cognitive Science and Psychology. Wilmington, Delaware: Vernon Press.

Douglas, Karen M., Robbie M. Sutton, and Aleksandra Cichocka. 2017. "The Psychology of Conspiracy Theories." Current Directions in Psychological Science 26 (6): 538–42. https://doi.org/10.1177/0963721417718261.

Fletcher, Richard. "The Truth behind Filter Bubbles: Bursting Some Myths." Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/risj-review/truth-behind-filter-bubbles-bursting-some-myths.

Fricker, Miranda. 2021. Epistemic Injustice : Power and the Ethics of Knowing. Oxford University Press. Accessed February 28. https://search.ebscohost.com/login.aspx?direct=true&db=cat00823a&AN=ceul.b1150622&site=eds-live

Fridman, Ariel, Rachel Gershon, and Ayelet Gneezy. 2021. "COVID-19 and Vaccine Hesitancy: A Longitudinal Study." PLOS ONE 16 (4): e0250123. https://doi.org/10.1371/journal.pone.0250123.

Giusti, Serena, and Elisa Piras. Democracy and Fake News: Information Manipulation and Post-truth Politics. London ; New York: Routledge, 2021

Grumbach, Jacob M. 2018. “From Backwaters to Major Policymakers: Policy Polarization in the States, 1970–2014.” Perspectives on Politics 16 (2): 416–35. https://doi.org/10.1017/S153759271700425X.
Guglielmi, Giorgia. 2020. “The Next-Generation Bots Interfering with the US Election.” Nature 587 (7832): 21–21. https://doi.org/10.1038/d41586-020-03034-5.
"Guidelines on Privacy and Online Behavioural Advertising." Guidelines on Privacy and Online Behavioural Advertising - Office of the Privacy Commissioner of Canada. December 17, 2015. https://www.priv.gc.ca/en/privacy-topics/advertising-and-marketing/behaviouraltargeted-advertising/gl_ba_1112/.
Haggerty, Kevin, and Richard Ericson. "The surveillant assemblage." British Journal of Sociology 51, no. 4 (2000): 605-22.
Haraway, Donna Jeanne. The Haraway Reader. New York: Routledge, 2004.
Hills, Filippo Menczer, Thomas. n.d. “Information Overload Helps Fake News Spread, and Social Media Knows It.” Scientific American. Accessed September 7, 2021. https://doi.org/10.1038/scientificamerican1220-54.
Hochschild, Arlie Russell. Strangers in Their Own Land: Anger and Mourning on the American Right. New York: New Press, 2018.
Hopp, Toby, Patrick Ferrucci, and Chris J Vargo. 2020. “Why Do People Share Ideologically Extreme, False, and Misleading Content on Social Media? A Self-Report and Trace Data–Based Analysis of Countermedia Content Dissemination on Facebook and Twitter.” Human Communication Research 46 (4): 357–84. https://doi.org/10.1093/hcr/hqz022.
"Individuals Using the Internet (% of Population)." Data. 2021. https://data.worldbank.org/indicator/IT.NET.USER.ZS.
Kevles, Daniel J. "From Eugenics to Patents: Genetics, Law, and Human Rights." Annals of Human Genetics 75, no. 3 (2011): 326-33.
Kitchens, Brent, Steve L. Johnson, and Peter Gray. "Understanding Echo Chambers and Filter Bubbles: The Impact of Social Media on Diversification and Partisan Shifts in News Consumption." MIS Quarterly 44, no. 4 (2020): 1619-649.
Lariviere, Christine. 2019. “The Fisher King: Solving Climate Change in a Post-Truth World.” Medium (blog). February 21, 2019. https://medium.com/@christinelariviere/the-fisher-king-solving-climate-change-in-a-post-truth-world-7b18c8eafd53.
Lee, Seung-yoon, and Contributor CEO of Byline. 400AD. “Julian Assange: ‘Western Civilization Has Produced a God, the God of Mass Surveillance.’” HuffPost. 54:37 400AD. https://www.huffpost.com/entry/julian-assange_1_b_7560710.
Lewontin, Richard C. Biology as Ideology. London: Penguin, 1993.
Lyon, David, Colin J. Bennett, Valerie M. Steeves, and Kevin D. Haggerty. Transparent Lives: Surveillance in Canada. Edmonton: AU Press, 2014.
Martin, Katherine Connor. 2017. “‘Post-Truth’ Enters Oxford English Dictionary.” POLITICO. June 27, 2017. https://www.politico.eu/article/post-truth-enters-oxford-english-dictionary/.
Marx, Paris. n.d. “Don’t Blame Social Media. Blame Capitalism.” Accessed September 30, 2021. https://jacobinmag.com/2020/09/social-media-platform-capitalism-the-social-dilemma.

Nightingale, Sophie J., Kimberley A. Wade, and Derrick G. Watson. 2017. “Can People Identify Original and Manipulated Photos of Real-World Scenes?” Cognitive Research: Principles and Implications 2 (1): 30. https://doi.org/10.1186/s41235-017-0067-2.

Orange, Michelle. 2019. “How Free Is Too Free? Surveillance Capitalism, Market Democracy, and the Dangers of Modern Freedom.” Virginia Quarterly Review 95 (2): 156–59. https://search.ebscohost.com/login.aspx?direct=true&db=edspmu&AN=edspmu.S2154693219100435&site=eds-live.

Pasquale, Frank. 2015. The black box society: The secret algorithms that control money and information. Cambridge: Harvard University Press.

“‘Post-Truth’ Enters Oxford English Dictionary.” 2017. POLITICO. June 27, 2017. https://www.politico.eu/article/post-truth-enters-oxford-english-dictionary/.

"Privacy Policy – Privacy & Terms – Google." Google. https://www.google.com/policies/privacy/.

Satz, Debra. Why Some Things Should Not Be for Sale: The Moral Limits of Markets. New York: Oxford University Press, 2012.

Scotto, Silvia Carolina. 2020. “Digital Identities and Epistemic Injustices.” Humana.Mente: Journal of Philosophical Studies 13 (37). https://search.ebscohost.com/login.aspx?direct=true&db=edsdoj&AN=edsdoj.56812ebc14674185b0b008183c5682f0&site=eds-live.

“Summary for Policymakers of IPCC Special Report on Global Warming of 1.5°C Approved by Governments — IPCC.” n.d. Accessed September 30, 2021. https://www.ipcc.ch/2018/10/08/summary-for-policymakers-of-ipcc-special-report-on-global-warming-of-1-5c-approved-by-governments/.

Sunstein, Cass R. Going to Extremes: How like Minds Unite and Divide. Oxford: Oxford University Press, 2011.

Ray, Tiernan. n.d. “Why Is Your Identity Trapped inside a Social Network?” ZDNet. Accessed September 21, 2021. https://www.zdnet.com/article/why-is-your-identity-trapped-inside-a-social-network/.

“The Tone of Social Media Discussions on Politics.” 2016. Pew Research Center: Internet, Science & Tech (blog). October 25, 2016. https://www.pewresearch.org/internet/2016/10/25/the-tone-of-social-media-discussions-around-politics/.

Turkle, Sherry, edited and with an introductory essay by. 2011. The Inner History of Devices. Cambridge, Massachusetts; London, England: The MIT Press. https://search.ebscohost.com/login.aspx?direct=true&db=edsjbk&AN=edsjbk.j.ctt166sb05&site=eds-live.

Turow, Joseph. The Daily You: How the New Advertising Industry Is Defining Your Identity and Your worth. New Haven, Conn.: Yale U, 2013. Print.

"Types of cookies used by Google – Privacy & Terms – Google." Google. https://www.google.com/policies/technologies/types/.

Wilkie, Rob. 2011. “The Digital Condition,” January. doi:10.26530/oapen_626991.

Wineburg, Sam, Stanford, and California 94305. n.d. “Evaluating Information: The Cornerstone of Civic Online Reasoning.”

"What Is Direct and Indirect Discrimination? | Equality and Human Rights Commission." n.d. Accessed September 30, 2021. https://www.equalityhumanrights.com/en/advice-and-guidance/what-direct-and-indirect-discrimination.

Zuboff, Shoshana. 2016. The Age of Surveillance Capitalism : The Fight for a Human Future at the New Frontier of Power. Profile Books. . https://search.ebscohost.com/login.aspx?direct=true&db=cat00823a&AN=ceul.b11411199&site=eds-live.