SURVEILLANCE CAPITALISM, THE COMMODIFICATION OF PERSONAL BEHAVIORAL DATA, AND HOW IT FACTORS INTO OUR RESPONSE

By

JULIAN HOPE WALLACE

A Thesis Submitted to the W.A. Franke Honors College
In Partial Fulfillment of the Bachelors degree
With Honors in
Political Science
THE UNIVERSITY OF ARIZONA
MAY 2022

Approved by:

Dr. Suzanne Dovi
Political Science, School of Art
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Context and History</td>
<td>5</td>
</tr>
<tr>
<td>The Issues with the Commodification of Personal Behavioral Data</td>
<td>10</td>
</tr>
<tr>
<td>What is Personal Behavioral Data and How Does it Work?</td>
<td>10</td>
</tr>
<tr>
<td>How is Personal Behavioral Data Commoditized?</td>
<td>14</td>
</tr>
<tr>
<td>Harm in the Process</td>
<td>16</td>
</tr>
<tr>
<td>Labor Exploitation</td>
<td>16</td>
</tr>
<tr>
<td>Privacy</td>
<td>18</td>
</tr>
<tr>
<td>Harm in the Aftermath</td>
<td>27</td>
</tr>
<tr>
<td>Constraining Choice</td>
<td>28</td>
</tr>
<tr>
<td>Nudging</td>
<td>31</td>
</tr>
<tr>
<td>Commodification: Attacking at the Source</td>
<td>34</td>
</tr>
<tr>
<td>Responses to Surveillance Capitalism, Shortcomings, and Revised Suggestion</td>
<td>35</td>
</tr>
<tr>
<td>The User-Centric Approach</td>
<td>35</td>
</tr>
<tr>
<td>The Third-Party Intervention Approach</td>
<td>38</td>
</tr>
<tr>
<td>The Governmental Approach</td>
<td>41</td>
</tr>
<tr>
<td>Policy Proposals</td>
<td>44</td>
</tr>
<tr>
<td>Conclusion</td>
<td>46</td>
</tr>
<tr>
<td>Works Cited</td>
<td>48</td>
</tr>
</tbody>
</table>
Abstract:

Shoshanna Zuboff jumpstarted a conversation about the dangers of surveillance capitalism. In the following years, many scholars have contributed to an expanding body of work, but many have failed to address the commodification of personal behavioral data (PBD). The process of commodification itself harms users, exploiting them and violating their privacy, but the true issue with this phenomenon is that it facilitates a future market where surveillance capitalist firms can trade predictions for future user behavior. This futures market encourages the use of behavioral modification. In order to prevent these outcomes, responses to surveillance capitalism must target commodification, which none do. This paper proposes that effective interventions will have to come from government, who will have to separate the profit-making and data-gathering aspects of surveillance corporations, in the tradition of investment adviser regulation.
Amazon’s third-party e-commerce platform was its second-largest source of revenue in 2021. It made $103.37 billion, a 28.5% increase compared to 2020, through charging third parties for shipping costs, referral fees, and fees for hosting their products on the Amazon marketplace (United States Securities and Exchange Commission 2021, p. 65). Amazon then uses data stored from third-party transactions to direct its own product development. Amazon claimed that they were using general trends in sales, but “in one instance, Amazon employees accessed documents and data about a bestselling car-trunk organizer sold by a third-party vendor…including total sales…and how much Amazon made on each sale. Amazon's private-label arm later introduced its own car-trunk organizers” (Mattioli 2020). Amazon will often even source directly from these companies' manufacturers, and thus “replicating the product under one of its private-label brands for a lower cost and siphon customers from the seller” (American Booksellers Association Advocacy Division 2021 p. 12). Despite public statements and testimony to Congress which denied these allegations, Amazon employees said that using third-party data in product development was “standard operating procedure” (Mattioli 2020). In harvesting and using the data left behind by business partners, Amazon has consistently been able to undersell them and encroach on their share of the market, slowly growing their dominance, and arguably monopoly, over aggregated e-commerce. Access to this information translates into increased market control and profit. This is the business model of the surveillance capitalist system: access data, run analytics, apply findings, and reap the profits. This process commodifies data and connects data gathering and profit-making as a joint enterprise.

This paper aims to do two major things. First, it attempts to outline how the commodification of personal behavioral data is harmful. This is a multi-step process that requires an explanation of how PBD is commoditized and uses several approaches to investigate the
potential consequences of this process. These approaches look at Marxist understandings of labor exploitation, commodification as an issue of human dignity, the limitations of datafying the human experience, social contract theory, and privacy concerns. That section's goal is to establish that commodification is an important part of the conversation about how we handle surveillance capitalism and the connected anxieties outlined above.

Second, the paper explores some possible ways to resist and ameliorate the harms inflicted by corporate surveillance and proposes some new policy options. In doing so, it exposes how little these solutions and countermeasures consider commodification. Here, the aim is to demonstrate that in failing to consider commodification, we fail to get at the heart of the issue: that our data is a tradable good. Without acknowledging and targeting this, we are unable to detect the structural relationship by which we lose our privacy and protect our freedom to choose. That is the foundation of the surveillance capitalist business model, so responses must target commodification if they would like to be effective in actually changing the system as it currently exists. I struggled to find proposals that I felt adequately addressed commodification, so I have also developed some additional suggestions for how we might begin responding to the whole issue, not just the symptoms.

**Context and History**

I offer a formal definition of surveillance capitalism. Shoshanna Zuboff (2019) offers a multipart definition on the inside cover of *The Age of Surveillance Capitalism* which includes the idea that surveillance capitalism is “a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales” and “as a significant threat to human nature in the twenty-first century as industrial capitalism was to the natural world in the nineteenth and twentieth.” That multi-part definition is extensive and details
facets of surveillance capitalism that this paper is not large or comprehensive enough to cover. Consequently, although I draw on some elements of her definition, I have both condensed and amended her definition for my purposes. In particular, I understand surveillance capitalism as a relatively new form of capitalism based on the internet and digital companies' ability to "claim human experience" and monetize behavioral data as a resource, which it then uses to predict actions and to sell more things to consumers. In addition, this form of capitalism doesn’t only track data but uses that data to predict (and influence) consumption. Surveillance capitalism converts the "behavioral surplus" derived from internet usage to manipulate and increase profits based on predictions and mass analytics.

Surveillance capitalism is a relatively "new evolution" of capitalism. Instead of coming into existence during the Industrial Revolution, surveillance capitalism has emerged in the last 15 years. This new economic system was based on the widespread use of computers and the internet and the massive exchange of data between individuals as a result. The addition of surveillance to the traditional capitalist model does not change the foundational aspects of the economic system: the goal is profit-making, first and foremost. However, in surveillance capitalism, there is a shift in the consumers of the products. The laborers are no longer also the consumers. In Marxist theory and according to Niamh Mulcahy (2016), laborers double as consumers because they become alienated from the fruits of their labor, and they cannot reap the benefits of their labor directly in a way that is sustainable for life. In contemporary surveillance capitalism, laborers double as consumers of secondary products, or the goods created by the consumers of surveillance capitalism’s primary products--access to functionalized personal data and a futures market. The products of surveillance are not sold to users, instead, users are “the means to
others’ ends” (Zuboff 2019a, p. 94). Thus, surveillance capitalism maintains the basic shape of the capitalist system and elongates it, emphasizing secondary and tertiary markets.

Surveillance capitalism has 4 goals: "data extraction and analysis,...monitoring, personalization and customization, and continuous experiments" (Zuboff 2019a, p. 64). The overarching purpose was to use the left behind data dubbed "behavioral surplus" to “predict and modify human behavior as a means to produce revenue and market control” (Zuboff 2015, Zuboff 2019a). The most common example of this is in targeted ads.

Initially, this information was used to increase the functionality of various companies' services (Zuboff 2019a, p. 69; Malmgren 2019 p. 44). The hope was to make products more reactive to user input, and therefore more useful (Malmgren 2019, p. 44). Zuboff calls it the “behavioral value reinvestment cycle”, through which user data analytics were all used to improve the user experience (Zuboff 2019a p. 69). For instance, in the early days of Google Search, the behavioral data gathered through the service was used by developers to improve the effectiveness of Search. Taking note of what people were most likely to search for, and what results were most useful to users allowed the company to figure out how to best present information and how to find people the search results they were looking for. Google “needed users as much as users needed Search” (Zuboff 2019a p. 70). However, these services were difficult to monetize, and this limited analysis of data exhaust was not a very profitable business model. In 2000, when venture capitalists started pulling their support from Silicon Valley start-ups in the "dot-com bust", the companies had to reconfigure themselves to create another revenue stream, one that uses the data to influence how people consume.

Surveillance capitalism started with Google’s AdSense department. In 2000 it was a highly successful search engine that was not making any money, and its investors threatened to
rescind their financial support unless they started making money (Zuboff 2019a, p. 73). So, the company had to start showing "sustained and exponential profits" (Zuboff 2019a, p. 74). Up until 2002, they were focused on monetizing their search engine, which had continued to grow in popularity and effectiveness. When they still had failed to start showcasing the money-making capacity that their investors demanded, they turned to the resource that was making their search engine so effective and decided to “commodify” behavioral surplus. This shift was a demonstrable movement away from the founders' initial promise and mission: to make the internet more accessible to people and to only use the behavioral surplus for the purpose of improving their search capabilities. With this new profit model, Google began gathering and monetizing data from their other fledgling services. Moreover, the business model spread quickly through Silicon Valley as other internet companies began taking cues from Google and monetizing the personal data of their users. Eventually, this financial model dominated the money-making approaches of most technology companies (Zuboff 2019a, p. 91-92).

Once Google combined its analyzing capabilities, access to behavioral surplus, and advertising, it had the foundations of surveillance capitalism in place. The financial model could save floundering companies in the red, and many jumped at the opportunity and converted their tech start-ups into surveillance institutions whose purpose was to provide data that would allow companies to predict and influence their clients’ behavior, which increases accuracy. Doing so required that companies get better at developing predictions of user decision-making, which in turn required an increasing amount of data to analyze. Zuboff (2019) called this "the extraction imperative" (p. 87). It motivated business moves like Facebook's acquisition of Oculus and WhatsApp, which although they were not profitable enterprises but contained vast amounts of user data (p. 87, 103). As a result, this iteration of the capitalist system attempted to use all the
behavioral data they could gather to predict our actions and desires in the present and the future (Zuboff 2019a). This is the fundamental logic of surveillance capitalism.

This became increasingly concerning to data experts and privacy researchers alike. Most notably Shoshanna Zuboff (2019a), chronicled the development of the system and detailed her concerns about free will, democracy, and the looming corporate overlords who knew everything about us. She called for drastic measures to safeguard what she described as "a human future" and protect against a world that would "strip personal life of whatever it is that makes it personal for you and me" (p. 63). Zuboff wrote as though the world was on fire or sinking into the ocean and it was surveillance capitalism's fault. The book fueled by anxiety about privacy concerns, data security, and a political climate influenced by businesses run on predicting and controlling behavior. With its publication, it triggered similar concerns in academics, researchers, industry professionals, and the general public.

This paper intends to build on Zuboff’s premise and argument\(^1\). The book and associated texts spend little time talking about commodification and offer solutions based on individuals' ability to circumvent or hide from surveillance, which she considers to be revolutionary acts (p. 488-492). This piece will attempt to explain why the commodification of PBD is harmful to

\(^1\) Despite her insights into the origins of surveillance capitalism, there are some flaws in the argument that she presents. Zuboff argues that surveillance capitalism is a wholly new phenomenon, novel because of the apparent indifference of consumers. In reality, "formal indifference is already the logic of capitalism" (Kapadia 2019, p. 339). Further, Zuboff occasionally overextends the argument and presents a "strange misreading of how capitalism actually works" (Breckenridge 2018, p. 6). There are also issues with her hyper-alarmism and occasional neo-liberal capitalist-apologist moment. Despite these pitfalls, the book is a testament to Zuboff's capabilities as a researcher and presents a thorough, comprehensive picture of how surveillance capitalism has come to exist while outlining some truly concerning potential impacts. While there is cause for concern, as this paper is further proof of, there is not a need for quite the panic that Zuboff approached the issue with. For instance, contrary to Zuboff's predictions, surveillance capitalists have yet to reach high levels of accuracy when predicting what we want and what our next choices will be.

Zuboff is also a fatalist, where I am not. She claims that surveillance capitalism has the capacity to fundamentally and negatively alter the entire landscape of humanity. I believe there are real concerns and real risks, but that there is also space and time for action. Humans are resourceful, enduring, and smart and capable of making real change in the systems that inform so much of our lives (Kapadia 2019)
individuals and society and will engage in discussion around how a community can respond. Zuboff offers some solutions and approaches to dealing with corporate surveillance, and I offer more in later sections of this research. There are clearly defined courses of action that are within the capabilities of individuals and countries to enact. We are not helpless at this moment, and now is not the time for immobilizing panic. Now is a time for action.

**The Issues with the Commodification of Personal Behavioral Data**

The commodification of personal behavioral data is step one in the surveillance capitalist process. The whole system relies on companies’ abilities to harvest data and convert it into something capable of predicting human behavior, thus commodifying it. The process of commodification creates an environment in which exploitive measures are acceptable in pursuit of this valuable resource, and it creates a futures market. The futures market is a world of predicted outcomes that various institutions are betting on. As a result, it is in every interest of both the companies using personal behavioral data for advertising, etc. and the companies harvesting the data to ensure the accuracy of their predictions, which requires more and more information. Speculation in a futures market entails some measure of risk, so it is logical to make interventions that might influence parties in your preferred direction. This is what we see happening with the constraint of choice and nudging.

**What is Personal Behavioral Data and How Does it Work?**

Personal behavioral data (PBD) can sometimes also be referred to as personal data, behavioral data, personal information, data exhaust, and behavioral surplus. It refers to the recorded and collected “facts” that individual users leave behind in their interactions on the internet: what they spend more time looking at, what type of content they interact with and how, when they are active, etc. This raw data is then compiled into big data. Big data typically
possesses four characteristics: volume, velocity, and variety (McAfee & Brynjolfsson 2012). Big data is both a technical term for data sets too big to be handled by common computers and, more importantly, a general term referring to the massive amounts of information available to surveillance capitalist firms. Using big data, one can find patterns in human behavior and learn to predict how individuals make choices. Almost any data point about someone’s actions while online is recorded as PBD. Personal data informs businesses about a person's attitudes, actions, habits, personality traits, and lived experiences. In the context of surveillance capitalism, PBD is used to predict what types of products and advertising will be compelling to users, thus making it more effective and profitable. At its core, PBD is information about who we are as people, made sellable and usable by Big Tech.

According to an article in the Harvard Business Review, one of the most cited articles on big data, it is data sets that are largely gleaned from internet activity that have three significant characteristics: high volume, high velocity, and high variety (McAfee & Brynjolfsson 2012). High volume is decently self-explanatory: it is simply an incomprehensible amount of data. In 2018, the internet created 2.5 quintillion bytes of data every day (Marr 2018), which should double every 40 months according to McAfee and Brynjolfsson (2013). High velocity would mean that the data is quickly gathered and analyzed. Think about Google Maps, which uses your GPS location, and the GPS location of everyone else on the road, to determine where there are slowdowns and how much time the additional traffic will add to your journey. High variety would refer to the diversity in types of information gathered, from GPS location to posts and interactions on social media, to messaging, even to biometrics (occasionally) (McAfee & Brynjolfsson 2012). Big data has exploded with the internet. The more time people spend online, and the better companies get at watching them while they are there, the more data there is to use.
This is synthesized (Zuboff 2019a). Data, in its initial form, is not useful to the surveillance capitalists because they need to know what that data means about human behavior. Thus, the raw data is worked over, made possible by the massive processing power available to companies like Google and Microsoft, and translated into recognizable and sellable patterns. At the source, all the surveillance provides is the facts of an interaction: Person A spent 15 seconds on this webpage, Person B clicked this link, and Person C played 87% of this video. This is raw data. When viewed in a broader context, in conjunction with other data points, one discovers that Person A spent 15 seconds on that webpage before they closed the tab, and they normally spent much more time on a webpage. Or Person B clicked on that link for the third time in the last 36 hours. Or Person C typically watches 55-90% of a video. All of this data is transformed into a story: Person A was less interested in that webpage than normal, Person B was more interested, and Person C was as interested as they typically are. That is PBD: information that tells us about how people act and respond. Now expand outward: there are hundreds and thousands of people interacting with the same sites the above people are, and those data sets are all combined, forming big data. After further analysis, we know that Person A was uninterested in the content on the webpage, and we also know that 64% of people fitting similar demographic characteristics, who also normally spend more time clicking through websites, were disinterested. So, we know that whatever the webpage was about is not compelling or interesting to people like Person A. Thus, we get insights into human behavior (Zuboff 2019a).

In the same article by McAfee and Brynjolfsson (2012), they talk about many of the categories that would come to be included under the PBD title. Companies take data points and transform them into PBD, then use them to create the ever-elusive algorithms that control so much of our digital interactions. They find patterns in the personal behavioral data that help them
to predict the outcomes of situations, or what a person might choose to do. For example, they might shift through their massive data banks and notice a trend: that people who tended to like more blue-toned pictures on Instagram were also more likely to look at blue tops while online shopping. So, when an Instagram user starts liking more blue-toned pictures, they might start making sure that the user sees more ads for blue shirts in their feed. Essentially, they gather enough PBD for it to be abstracted into patterns of behavior, which is modeled in an algorithm, which is then applied to the individual user in this cycle of zooming out and then zooming back in. This is how surveillance capitalism makes its money.

There are very valid concerns that start to appear at this junction. Since people have been shown time and time again to be highly susceptible to interference from outside sources in their decision making such as through advertising and nudging (Thaler & Sunstein 2008), there are very real fears that surveillance capitalist firms could start not only predicting the choices of consumers but *influencing* them or even controlling them (Zuboff 2019a). It’s a potential not-so-distant future that we may be seeing the beginnings of in the present. It could have long-lasting impacts on conversations and research about social conformity, hegemony, democracy, and free will to name a few (Zuboff 2019a).

**How is Personal Behavioral Data Commoditized?**

---

2 Thaler and Sunstein’s 2008 book *Nudge: Improving Decisions About Health, Wealth, and Happiness* effectively informed academics and the general public of the potential impacts of “choice architects”. They explored how choices could be influenced by small nudges in one direction or another. For example, putting fries at eye level versus higher or in a different line could influence school children’s likelihood to eat them by up to 25%. To use a more applicable example, we see a similar phenomenon happen with fashion trends. The more times people see a trend, the more likely they are to like the style and buy clothes to conform to said aesthetic. I, for one, really used to hate bike shorts and now I own two pairs. By putting this style in front of me often enough, the internet convinced me that they were cute, and I spent upwards of 60 dollars on the pairs that I bought from an online thrift store. I also became interested in it after seeing ads for it over and over again. We see nudging all the time, in so many of our small decisions.
My concerns are more specific in the foundations for this phenomenon. Personal behavioral data, on its own, is not worth very much. The process of compiling massive amounts of PBD, analyzing it, turning it into an algorithm, and then using the algorithm to market to users makes PBD highly valuable. In 2021, Google made $61,239,000,000 in ad revenue. Google as a whole made $75,325,000,000. This is just under a 33% increase from the previous year’s ad revenue (Alphabet 2021). This is a growing industry, and it has been since the advent of surveillance capitalism in the mid-2000s. Without access to personal behavioral data, this level of earnings would be impossible, meaning that PBD is worth a lot to companies like Alphabet and Meta and it is a cornerstone of their profitability.

Commodification is a transformative process through which something that previously had no market or exchange value becomes valuable to the market. There is a negative connotation associated with the word; many find the process of commodification to be reductive in that it takes things with inherent and intrinsic value and treats them as “mere objects” (Maloney 2020 p. 1). Commodification objectifies, in a more literal sense. By attributing economic worth to something that would not traditionally be valued in that manner, capitalism and the market are able to absorb and manage the thing. Commodification is a broad phenomenon experienced by land and nature, the human body, goods and services, and now PBD.

In order to have access to this resource, surveillance capitalist firms acquire this resource by exchanging it for services that users want (Zuboff 2019a). For example, Google Search funnels information about what sites people are interested in into their advertising department. Google's search engine serves multiple functions: it both is the mode through which data is

---

3 This is one of the issues that I address later in the paper when I talk about solutions to personal behavioral data.
gathered, and the reward that users get for "allowing" access to that same data. Google improves user services and includes new ones as rewards for using them and letting the company have the users' PBD (Zuboff 2019a). Or look at Facebook. Facebook gathers information by monitoring how people interact with the social media platform and rewards users with an improved platform and free access to the social networking site. This is an exchange. Because personal behavioral data is so valuable and so critical to the profitability of surveillance capitalist companies, they are willing to pay for the development and management of their platforms and services and give them to users for free. Except, it's not really for free, it is in exchange for their internet traffic and the information they leave behind about their interests and lives. Thus, PBD is not only invaluable to these companies, but it also is a source of.

Commodification is the process through which something becomes a good that can be bought or sold or traded. Commodities are broadly defined as “objects of economic value" (Appadurai 2014). According to George Simmel, “objects traded are made valuable by the exchange,” meaning that procedure of trading a good for something else imbues that object with value. In a word, “exchange is not a by-product of the mutual valuation of objects, but its source." (Simmel 1978). Marx agrees and claims "that a commodity is an object primarily intended for exchange" (Appadurai 2014, Marx 2000). Thus, commodification is the process through which something is made accessible to markets, and thus possible to exchange. In most contexts, commodification is associated with the devaluing and objectification of things with intrinsic value to people, though not to markets. For example, it is commonly used when discussing environmental concerns. The commodification of different environmental elements makes them market accessible, and therefore also making them more easily degraded should it be profitable. Seen as a unique and independent entities and resources within the context of
market exchange, commodities are removed from their context regardless of the impacts on said context (Death 2013).

Personal behavioral data is made into a commodity because surveillance capitalist companies find it valuable and are willing to exchange their services in payment. PBD is then isolated from its context as information about personal activities and preferences, and made compressible for a capitalist context, where it will be valued by how much someone is willing to pay for it. Personal behavioral data, without the intervention of surveillance capitalism, is nothing. PBD is the information and data points gathered by surveillance capitalism, and without that, PBD is just our lives and interests. When surveillance capitalism started to monetize and value the information about human behavior that they could glean from our internet traffic, it created a commodity from the bits and pieces of behavioral surplus that users did not have an awareness of and that few had cared about up until this point.

**Harm in the Process**

*Labor Exploitation*

Marx argues in his labor theory of value that profit is made in the space between the value that is created by a person’s labor, and what they are paid (Cohen 1979, Marx 1935). The foundations of capitalism are, therefore, exploitation of the labor force through increasingly lower wages. Though scrolling through your Twitter feed likely does not feel like labor, it nonetheless is producing a raw material that can be used by companies. A tree in the forest is a raw material, but it is not usable until someone puts in the labor of cutting it down. Minerals in a mine are worth something only if there are also miners who are willing and able to tunnel down and bring them up. In the same way, personal behavioral data has always existed because it is derived from our behavior, and we have always made actions. Therefore, personal behavioral
data has always existed in that undiscovered, untouched sections of old-growth forests exist: we know they exist but we have no way of using those raw materials until we have the necessary resources and labor to retrieve them. Technological advancement and the establishment of the surveillance capitalism framework discovered the forest, and users interacting with sites like Facebook or Google Search metaphorically felt the trees. There are, of course, many laborers who create many different versions of the material before it becomes its final form, but the labor at each stage in the process is still labor. Thus, even though more labor goes into transforming PBD into an algorithm capable of highly targeted ads, the process of providing the personal behavioral data and of making it available to companies remains the initial labor.

As such, it is compensated. The payment in this case is free access to the sites that harvest PBD. There are notable benefits to this. Social networking and social media have had massive impacts on pop culture, and being tapped in allows people to educate themselves, advertise, mobilize, interact with friends and families, and discover communities that they would have been cut off from otherwise. I have no wish to deprecate the impact or the worth of access to social media and other web-based services. However, it is doubtful that the value of the services we have access to is equivalent to the $20 million that Instagram, for example, made in revenue in 2019, or the estimated $26.46 billion it made in ad revenue alone in 2021 (Statista 2022). If we accept the Marxist premise that profit is made in the space made by not paying laborers equivalent to the value that they create, then it can be extended to this situation, and we can recognize the similar exploitation between the gathering of PBD via internet traffic and wage theft. To many, the act of trading that information away resembles trading away parts of themselves. In Sebastian Sevignani’s research on the commodification of privacy and personal data, they claimed that it was a "form of selling my own self" (2013).
Commodification creates a good out of the information that can be surmised from the left behind data points on the internet. In the process, the people creating those data points not only become the targets for the final product of the larger surveillance capitalist system, but they become the initial laborers providing it. For their work, they are rewarded with services designed to draw them back in and keep them by providing more data and feelings of violation. The process of creating commodities of PBD is fundamentally extractive and exploitative. Eric Schroeder from Bethesda, MD wrote to the NYTimes and summed up the feeling this can elicit:

Perhaps the voluminous terms and conditions that are required to be acknowledged by users of internet services can be made more succinct by simply having the tech companies state the obvious in one sentence: “We, (Giant Internet Corporation), intend to exploit and profit from extracting every bit of personal data that can be gleaned from your online activities; we are not responsible, nor can we be held accountable, for any consequences that result from this intrusion into your privacy (2021).

**Privacy**

The process of commodification also produces concerns about privacy. One of the flaws of privacy, as something to be protected and as a discussion topic, is that “there is little agreement on how to define privacy” (Moore 2008, p. 411). Depending on the social, cultural, governmental, and legal environment, the definition shifts, and warps (Westin 2003). This makes it difficult to determine what, exactly, is technically private and what is public. The courts define privacy through the parent-doctor relationships, William Parent thinks about privacy in terms of “control over information about oneself”, Westin adds an argument for the control of how that information is used, and Moore talks about privacy as “the ability to control the access others
have to us” (Westin 2003, Parent 1983, Moore 2008, DeCrew 2018). For any of these approaches, personal behavioral data would be considered private.

One definition of privacy comes from legal sources. Such a definition is framed in terms of the doctor/patient relationship. Medical ethics consistently values privacy, as “respect for privacy and confidentiality has…been a responsibility of the physicians throughout history” (Humayun et al. 2008). The emphasis is on protecting the medical professional relationship so that the dignity of patients is preserved because “privacy and dignity are interlinking concepts” (Whitehead & Wheeler 2008). Medical practice often requires patients to make “a full and frank disclosure…of intimate, personal, and private information,” a description that is quite similar to William Parent’s definition of personal information (Challener 1950, p. 624). Medical history questionnaires, which are required in by most medical practices, will ask patients about their home life, their occupation, their childhood illnesses, whether or not they were adopted, what medications they take, their sexual activity, their exercise, and diet, how much they drink or smoke, and on and on (TriHealth 2012). This information is required before a patient even has the chance to talk to a physician about any health concerns. All of this is about a patient’s life choices and behaviors that they might not want available to the public, and as such is protected by patient confidentiality provisions (Challener 1950). A medical practice requires much of this information to provide quality care and treat patients, but it recognizes the power asymmetry and vulnerability created by the disclosure and has the precedent to back it up.

These statutes have been the precedent for much of the privacy protections we see in the legal code of the US. But the definition has distinctive limitations for context outside of the legal system. In contrast, personal behavioral data is not specific to the information required to make

---

4 Admittedly, the legal definition of privacy presented in this section is limited to the United States, as the laws, precedent, and courts discussed are also limited to the US.
accurate medical diagnoses and provide adequate care. Instead, it the broader umbrella under which much of the information contained by medical history forms falls. The information requested is about individual behavior (smoking and drinking, sexual history, exercise, and diet) that would also be of interest to surveillance capitalism. Internet companies are interested in more that the behavior that would directly impact one’s physical state, including their interests and attitudes). But medical practice and surveillance capitalism have similarity in that they need sensitive, deeply personal and specific information about individual’s actions in order to do their job. Thus, we can determine that a significant portion of the data that surveillance capitalism gathers could legally be considered private information. If the information disclosure to medical professionals creates a large enough vulnerability on the part of the disclosure that it is carefully protected, then there should be similar protections on the information harvested by surveillance capitalist firms.

Still using medical practice as the backdrop, many legal scholars make an argument for a right to privacy. Formalized in *Griswold v. Connecticut* (1967), the Supreme Court recognized the privacy as protecting “the social institution of marriage and the sexual relations of married persons” (DeCrew 2018). The Court decided that “‘Privacy involves the choice of the individual to disclose or to reveal what he believes, what he thinks, what he possesses” (Zuboff 2019a p. 89-90). This has expanded over the subsequent years, encompassing landmark cases like *Roe v Wade* and anti-sodomy cases across the United States. This conception of privacy is focused on intimacy, and personal autonomy within the confines of the “private sphere” (DeCrew 2018). This is the right to act in accordance with your own will, without onlookers. It makes provisions for divisions between the public and private personas, which can be applied to the concept of PBD. Commodities, due to their contextual nature as a good, are
inherently public facing because they must be able to be traded on the market⁵. The right to privacy outlined here is limited in scope, but it refers to an entitlement to have some behaviors and interests be shielded from public consumption at the discretion of the individual. If this attitude is extrapolated, then there is an argument to be made for a right to privacy precedent protecting PBD as well, since the majority of it is harvested from personal devices and can reveal information about non-public facing actions and attitudes.

More theoretically and philosophically, Parent defines privacy as “the condition of not having undocumented personal knowledge about one possessed by others” (1983, p. 269). They then go on to define personal information as “facts about which a particular individual is acutely sensitive and which he therefore does not choose to reveal about himself” (1983, p. 270). For Parent, privacy is the right to not have other people know things about you that you do not want them to know. This is difficult to assess in an impartial, socially universalist manner as it is deeply dependent on the socio-cultural context. What is embarrassing or dangerous information about a person in one context might be inconsequential in another. Thus, privacy is control over “significant personal matters,” whatever those might be (Parent 1983, p. 272).

In contrast, Alan Westin argues that privacy is control over “when such information will be obtained and what uses will be made of it by others” (2003, p. 431). The defining characteristic of privacy requires being able to have some measure of control. To protect their privacy, a person must be able to have access to and deny access to others the relevant details about themselves. This could mean telling no one, or it could mean publishing a dramatic autobiography with it all on display. Those decisions might change over time. As Westin wrote, “In these states of privacy, the individual’s needs are constantly changing…Such changing

---

⁵ It is a part of market language. When a company goes “public” that means its stocks are available for purchase and subsequent exchange.
personal needs and choices about self-revelation are what make privacy such a complex condition, and a matter of personal choice” (1998, p. 433-434). Thus, Westin addresses the autonomy of the individual and its centrality to his conceptualization of privacy. If one accepts the definitions of Westin and Parent on privacy, then it is important to determine where and if surveillance capitalism infringes on the control and autonomy of individuals.

However, if privacy requires individuals to control how their information is handled, disseminated, and used, then most surveillance capitalist action is in direct opposition. Once information is gathered, there is extraordinarily little transparency about how companies are going to use it (Zuboff 2019a). The assumption is that the information will be used to improve advertising campaigns, but as this research has explored, it could be used to affect user behavior and choices without permission and such use is a clear violation of Westin and Parent’s definition of privacy. There is a counterargument to be made that in including terms and conditions contracts and asking for permission to use cookies, etc., surveillance capitalism effectively covers its bases. But, as this research has already discussed, those contracts are exploitative, and consent is almost always given with little to no awareness of the contents of the contracts. If companies are intentionally making it difficult to avoid assenting to surveillance or to be aware of what using their services would entail for the user, then the legitimate authority has not been granted.

Adam Moore offered another way of understanding privacy. He defines privacy as “a right to control access to places and ideas independent of instantiation” (2008, p. 418). To apply this way of thinking to the issue at hand, one would have to support the idea that the commodification of personal behavioral data would supersede the ability of individuals to be able to control who has access to their information. While remarkably like the construction of
privacy used by Parent and Westin, it is less concerned with the condition of knowing, and more concerned with the condition of having. Being able to control who knows what about you is an issue of a stranger knowing that you like pineapple on your pizza while controlling who has access to that information is an issue of a stranger being able to find out that you like pineapple on your pizza. In many ways, this is again, a step further than the thinking of Westin and Parent. It extends what qualifies as private to contain the process through which a person could have information revealed. There is still a significant control aspect here in that Moore is talking in terms of restricting access to oneself (2008). Privacy “obtains” the condition of preventing others from having access (Moore 2008, p. 417). In such a space, the qualifications of being able to control who knows what about you, and how that information is used, are assumed. This “affords control over ideas no matter how these ideas are instantiated”, thus making sure that no matter how information is stored or presented, it is in the full control of the subject.

As we previously established, PBD is the information gathered by companies about a user's interests, activities, life events, etc. The goal is to know as much about people as possible to anticipate their choices, further to market to them better, and nudge their choices more effectively. This means that surveillance is not skipping over the sections of individuals' personal information that they would prefer to be kept private. In creating a system that prioritizes the massive gathering of data because it has been translated into something valuable, surveillance capitalism has stated that privacy is not a concern of theirs. In commoditizing personal behavioral data, they have commoditized some of the critical components that make up privacy. One could argue that due to the depersonalization of data, this information cannot be tied to an individual, and therefore is not an invasion of their privacy. Unfortunately, that is not true. Commodified data available to the public for advertising or personal use through data brokers is
incredibly easy to decipher and thereby link to a particular person (Oliver 2022). Additionally, this still does not change the fact that this information is accessed, nonconsensually, in the first place. If privacy is a measure of control, if it entails being able to regulate who has what information about you, then even this harvesting of PBD and accessing of your data is potentially a violation of privacy.

Surveillance capitalism, in its very foundation, needs easy access to information. Once again, someone could argue that we consent to the ubiquitous access that surveillance capitalism demands when we select the "accept all" button in the pop-up at the bottom of our browser. Technically, we consent to vague terms, but this is not an informed decision or easily avoidable. These contracts are highly exploitative. Researchers with Carnegie Mellon did the math in 2008 and found that it would take 76 business days, or 15 business weeks, to read all the important terms and conditions that you come across in a year of interacting with the internet. If you just skimmed them, it would take 25 days and the national opportunity cost would have been $781 trillion which is about equivalent to the GDP of Florida (McDonald & Cranor 2008, Madrigal 2012). They are too large to sort through, and they are too complicated for those without a legal background to follow, intentionally. The Boston Law Review investigated the language in these contracts in 2019 and argued that they placed an undue burden on the consumer, not only to read them but to understand them. The recommended reading level for public-facing writing is around the 6th-8th grade while most of these would require at least some college to understand and mimic the style of academic journals (Benoliel & Becher 2019). There are massive blanket clauses that cover almost anything that these companies could do and are subject to change at any point. They have used the terms and conditions to work around local privacy laws and to
regulate how people can interact with their services. This approach renders any attempt at getting legitimate access to PBD spurious.

Further, some firms are gathering data even when that access is explicitly denied. The Associated Press reported in 2018 that Google “some Google apps automatically store time-stamped location data without asking”, even when a phone’s owner has turned off location sharing (Nakashima). Deleting this data is possible, but it follows the pattern established by their public-facing contracts: it is laborious, “painstaking,” convoluted, and requires some level of expert knowledge (Nakashima 2018). This consistency in approach by surveillance capitalist firms reveals an attitude about PBD, and how little concern is spared for the sources of that information. These are intentional choices made by companies to keep users in the dark about how much information they are gathering, and it takes advantage of user trust, dependence on their services, and limited awareness of how much access they have to users’ lives.

Clearly, that "accept all" button does not constitute legitimate assent. John Oliver recently exposed how much information can be gained by companies from just being on a website where they have access to the data. They can see what else is happening on your computer, where you have been, and more (Oliver 2022). Even if you decide that you would agree to let a company surveil you, in exchange for whatever they are offering, they will have gained access to many spaces that you did not agree to. Unfortunately, with the way the internet is structured, it is incredibly difficult to prevent yourself from leaving behind data exhaust or to grant these companies only limited access (Oliver 2022, Zuboff 2019a). Being on the internet, which is required for many people, means that any number of unknown companies and organizations will have nearly unrestricted access to everything, whether you know it or not. Limiting access is the first line of defense to preventing the invasions of privacy associated with knowing things you
would rather they not know and with knowing how they are using that information. Companies and individuals cannot know anything they are not supposed to or do anything with that information if they cannot gain access to that information in the first place.

Thus, the commodification of personal behavioral data is a privacy failure, which has broad and wide-reaching impacts. As discussed by Parent, personal information is often a source of great discomfort and embarrassment to individuals, and the disclosure of it can feel like a violation of intimacy or a breach of boundaries (Challener 1950; Parent 1983; Moore 2008). Thus, maintaining privacy becomes an issue of “human dignity, freedom and independence” (Lukács 2016). Much like the commodification of personal behavioral data, disregarding privacy is degrading to the individual and destructive to places of seclusion and safety, where a person may be a person. We often talk about the “right to privacy” because many legal scholars and theorists see this ability to control the information about oneself to be part of our needs as people.

Finally, privacy is often a safety or a well-being concern. For example, privacy has been used to protect the queer community consistently, and violations of privacy often put people in danger (Samar 1991; THE REST). Outing someone to their family or school has often resulted in intense bullying, being kicked out of their home, or attempts to "turn" queer kids straight. In the workplace, it might result in discrimination, or in the case of a priest who was discovered to be gay through his internet usage, it meant losing his job and being expelled from the religious order to which he had devoted his adult life (Oliver 2022). Privacy is security in these situations and the legal framework that has been used to advance the rights of queer people (Epstein 2002). In a world that is inhospitable and dangerous, being able to retreat into privacy can be lifesaving. For victims of violence, who are fleeing homes and situations where they are in jeopardy, being
able to maintain anonymity and control who has access to their information is also an issue of safety. If a person's abuser can access all their information, it makes it nearly impossible to hide (Oliver 2022).

Surveillance capitalists have no issues with pushing aside privacy concerns. In fact, Mark Zuckerberg said in an interview in 2010 that he was able to establish new attitudes about privacy and that privacy, as we understand, no longer existed (Kirkpatrick 2010). He claimed that he was able to make privacy whatever he needed it to be for his business to be successful. In commodifying PBD, surveillance capitalist firms degrade privacy protections. The process itself causes harm to users by capitalizing on user’s cultivated ignorance and dependence on internet services. To prevent this injury to individuals, and society at large, interventions must happen at the point of commodification. Without considering the impacts of transformed PBD, potential solutions and responses fail to protect essential social norms and rights of humanity.

Harm in the Aftermath

A futures market is a term coined in the stock market and refers the place where future contracts are exchanged. Future contracts are “an agreement between two parties to buy or sell an asset at a certain time in the future for a certain price.” (Hull 2015, Kariya & Liu 2003). It is like purchasing an IOU, or a promise for a good or stock to be delivered in the future. For the purposes of this paper, a futures market will be defined as the market where predictions are sold. Though less stable than the derivatives or contracts sold in traditional stock markets, predictions of user behavior are bets on an individual’s actions. My version of a futures market is the trade of what companies think users might do in the future or in the present. This future remains theoretical and changeable, based on PBD analysis, and thus flawed. However, should the predictions be correct, both sides of the transaction will make a significant profit, so exchange in
and accuracy of these futures is also highly valuable. Resultant to the profit at stake, surveillance capitalist firms and their consumers (advertisers) are willing to engage in behavior modification such as constraining choice or nudging. Commodifying PBD creates this futures market by allowing for the creation of predictions. This futures market, retroactively, is part of what makes PBD worth something.

**Constraining Choice**

As a result of commodification and the subsequent simplification, we are categorized and targeted. Advertising through something like Google's AdSense is incredibly simple and available to anyone at any time. To experiment, I created an ad for my local roller derby league. I was able to select keywords and themes, as well as location. I was able to select within 5 miles of the campus and target people looking for derby gear, skate parks, Tucson Roller Derby, and collegiate sports. Anyone who would be interacting with any of those categories has the possibility of seeing our ad pop up on a Google ad platform. This means that anyone who fits into any of the categories that I mentioned is decently likely to have my ad presented to them as an option in their internet surfing.

Say that the other local and state leagues had a similar idea and started advertising with Google. They might have slightly different keywords or a broader target distance, but there would be significant overlap. Now maybe an individual would be interested in my team, but they did not specify collegiate derby, or they were looking for short-track instead of flat-track derby, but they would have been open to joining our team had it been presented as an option. So, they get ads for Copper State's webpage, and they do not take the time to dig around and see who else might have a team they could join, so they end up becoming a member of Copper State when they could have been equally happy with us at the Derby Cats.
It can be difficult to understand why a company might present limited options when the internet is infamous for its depth and breadth. However, surveillance capitalist firms gain access to our data, which is necessary for them to make the predictions about our future behavior and thereby how we will interact with their services. The longer, and the more often, users access the goods and services of companies like Google, Microsoft, and Meta, the more information they gather and the more effective they become at both predicting user decisions, and the user connected. So, they use past and present interactions from users with similar demographic markers to show users what they think they will want to see.

This expands beyond advertising and can affect things like Search results. For the inexperienced home cook, Google is an essential resource for finding recipes. The ranking system on Google’s website is based on internet traffic, meaning that the more people click on it, the higher it will be in the search results, or more likely it is to be eye-catchingly presented in rotating “carousels” at the top of the results page (Dewey 2020). So, more people will click on it and the higher it will climb. This diminishes the regional and international diversity of flavor profiles and could create a “massive lot of food culture” (Forum for Philosophy 2021). The internet is full of recipes, and everyone is making the same New York Times or AllRecipes.com version of chocolate chip cookies, or barbeque, or cassoulet (Forum for Philosophy 2021, Dewey 2020). Food is homogenizing because of the way that the recipes are structured, e.g. which recipe appears first and which recipe has more likes, and food homogeneity is good for Google because it allows them to charge advertisers based on the anticipated number of viewers. It means Google will be able to send you the recipe you want, right off the bat, every time. Limiting options, quickly or slowly over time, increases accuracy of their predictions because
they can more easily reproduce a user's choice if the user has essentially more difficult alternative options.

Additionally, constraining choice by limiting the number of available choices infringes on individual and collective freedoms. If freedom is the ability to make better choice options, then surveillance capitalism also infringes on freedom. Surveillance capitalist firms are not concerned with better, only consistent, and replicable. If these companies are deciding what the available options are for a decision, then they limit the market’s ability to furnish consumers with a variety of options and let them choose. The market cannot improve people’s choice options without surveillance capitalist support, regardless of the quality of the option they represent. So, though one might expect surveillance capitalism and the internet to broaden an individual's options by presenting new and unheard-of ones, the process is more like a curation, with no available exit.

This is a consequence of the commodification of PBD. The situation explored above limits someone's available choices due to how an individual is assumed to behave, thus constraining their future and present behavior. Behavioral constraints make it easier to predict future actions because it limits the viable options for those actions that can replicate past ones, which makes surveillance capitalist companies richer and richer as they engage in future market exchange (Zuboff 2019a). This is not possible without the creation of such a market or without the data necessary to create the choice constraints in the first place. Both facilitating factors are derived from commodified personal behavioral data. The capabilities and environments made possible by commodification are part of what makes PBD valuable and motivates the process in the first place. Data is used to categorize us, which is used to create profiles of forecasted decision-making (Zuboff 2019a). The specifics of those categories allow advertisers to be highly
effective in structuring and thereby constraining user choice to the ones that are going to make money: the choices they predicted users would make. The more about people that they can ‘buy,’ the more efficient this process becomes.

**Nudging**

Another concern is nudging. Nudges are pieces of "choice architecture that alter people's behavior predictably without forbidding any options or significantly changing their economic incentives" (Thaler and Sunstein 2008 p. 6). Whether or not you agree with Thaler and Sunstein’s book Nudge and think that we should guide people in a direction that is "good" for them, there is well-established evidence that the presentation of choices can change the choices that we make. Human beings are incredibly easy to manipulate and the way that options are presented, in space, in a specific order, whether something is an opt-in or opt-out, all have a significant impact on the choices we make. It is reminiscent of the idea of subliminal messaging and advertising, which was a Cold War "idea…that unscrupulous businessmen could make unwary customers buy more products simply by flashing visually undetectable…images" (Leonard 2008). The most common example of subliminal advertising is an experiment from the 50s where movie theaters would project a split-second image of the words "buy popcorn" in the middle of a film, with the hope of driving up popcorn sales. The thought was that the message would subtly prompt patrons to get up and head to concessions.

Subliminal advertising was quickly proven to have little to no effect on the choice behavior of experimental consumers (Theus 1994, Trappey 1996). However, nudging has been found to have a "median relative effect size of 21%" and an average effect size of 30%, when outliers were removed (Hummel & Maedche 2019). Digital nudging, which is the nudging that advertisers would be implementing using gathered PBD, nudges that "[involve] user-interface
design elements", like social media ads, the design of a user interface like a search engine or the default settings of such a setting. Digital nudges were found to be as effective as non-digital nudging (Hummel & Maedche 2019). What is most concerning about nudging, as it relates to surveillance capitalism and the commodification of PBD, is that it is a possibility. Currently, we have yet to see much research establishing that nudging advertising activity has been as effective as Zuboff and others claim or are concerned about.

We see nudging in two ways in surveillance capitalist spaces. The Netflix film/documentary "The Social Dilemma", talks about nudging in push notifications, urging people to re-engage with social media based on their previous interactions with the app (Orlowski 2020). Nudging can also occur in less obvious contexts, like in the it-game of summer 2016 Pokémon GO which allows companies to influence the geographical location of critical aspects of gameplay in the hopes of bringing in more foot traffic (Zuboff 2019a) and states that "information that we collect from our users, including Personal Data, is a business asset" (Niantic 2021). By encouraging people to spend more time traipsing across their city trying to catch a Charizard or prompting them to jump back onto their Instagram feed for a minute to check out a post from a friend, these companies can gather more data. As previously established, since PBD has been commoditized, it has become a very valuable resource and nudging can be a tool for extracting said resource.

Additionally, we can see nudging in the advertising itself. There is a lot of ongoing research, particularly in the field of digital nudging, and a significant amount of disagreement about its effectiveness and ability to change behaviors. Hummel & Maedche’s (2019), "How effective is nudging? A quantitative review” investigated 100 studies on nudging and their reported impacts on decision-making to discover how much influence nudging has. In the end,
they called for further research and interest, because despite it being "less effective than proclaimed", it can often have a statistically significant impact on the choices of individuals. (Hummel & Maedche 2019). Nudging might not need to be a source of anxiety in itself, but it is indicative of a larger attitude, which is cause for concern. Business executives, advertisers, data brokers, and choice architects, are all willing to try and change our behaviors. The point of surveillance capitalism is to know enough about you, and enough about people in general, that you can predict and capitalize on those behaviors. Nudging takes it a step further and tries to influence those behaviors.

This is another point where much of the existing work on surveillance capitalism begins to discuss issues with governance and with fascism and any number of frightening things that might be easier in a setting like this. When businesses can nudge people with a lot of success, they have an inordinate amount of power and influence over the institutions, beyond our behaviors, because it could affect things like voting or a person's opinions on an impossible number of sociopolitical issues. This fear is a concerning potential reality that has caused many thinkers to ring the warning bell. Shoshanna Zuboff has been one of the most prominent people talking about the impacts of surveillance capitalism's capacity for behavioral modification and what that means for democracy. At points, the book reads fatalist and alarmist, though this piece in no way aims to undermine the anxiety or concern associated with these dystopian futures. However, it hoped to explicate some measures governments and societies can take to minimize and prevent a lot of the harm discussed here. To do so, we must first recognize that the process

---

6 It is worth noting, however, that the abilities of surveillance capitalism are, at this time, somewhat limited both by their capacity and by external forces regulating their behavior. As noted earlier, the amount that individuals can be swayed by nudging is small, and likely overestimated (Breckenridge 2018). However, the capabilities exist and there exists a possibility that surveillance firms might become more and more effective. Making an intervention into the commodification of PBD now is thus a preventative measure.
of commoditizing personal behavior data makes all of these horror stories a possibility. In making PBD a commodity, the market and Silicon Valley have created a system intent on gathering as much information about users as possible so that their predictions can be as accurate as possible, and which makes this information available for misuse in pursuit of success on the futures market.

**Commodification: Attacking at the Source**

Commodification establishes that personal behavioral data is a free game and can be gathered without any of the protections that intervene in law enforcement surveillance\(^7\), or doctor-patient relationships, because it is like any other resource. Because PBD is a resource, and an intermediary good, it is valuable to own or have access to. But users do not own their information, and personal behavioral data becomes a business asset of these corporations and data conglomerates. This way of codifying who “owns” the data neatly establishes that our digital interactions and the information that can be harvested and become the possession of the companies we interact with, regardless of how personal or intimate the information, or of user discomfort with that information being public. The process of commodification invades privacy and distances users from control mechanisms over their information while exploiting their labor in providing the data. Further, commodifying personal behavioral data advances the forecasting proficiency of corporate surveillance firms, thus making them competitive in a futures market. The futures market, in turn, motivates moves in behavioral modification to ensure the accuracy of their predictions. This harms users by limiting choice, and through choice freedom, and by

---

\(^7\) Actually, law enforcement can just buy access to surveillance capitalist data and circumvent the need for search warrants (Oliver 2022). So corporate surveillance is often also government surveillance. So much so that Google has been an FBI contractor since 2004 (Zuboff 2019a).
controlling action through nudging. Effectively attacking these effects requires that intervention be made at the source: commodification.

**Responses to Surveillance Capitalism, Shortcomings, and Revised Suggestions**

The sudden and dramatic rise of surveillance capitalism has left many confused about what should be done. In response to concerns about “nudging”, behavioral changes, free will, freedom of speech, and the legitimacy of democracy, several avenues to mitigating the danger of surveillance capitalism have been proposed. In particular, there are three main approaches: 1) consumer boycotts of predatory companies 2) interventions by third parties which would safeguard greater user agency, and 3) governmental interventions that limit the power of big data.

**The User-Centric Approach**

Collective action can fail for many reasons. This paper will highlight two: failing to mobilize a significant enough portion of the populace who would be able to act against surveillance companies that their exit would impact profits, and by not having bargaining power, Before the COVID19 pandemic, the internet was essential to work, socializing, and learning for many Americans. Now, we find it even more critical to our lives. In April of 2020, mere months into the pandemic, 87% of Americans found internet access highly important to their lives (Vogels, et al. 2020). During the same month, 94% of parents with children in K-12 reported that their children's school had closed and that instruction had moved online, inciting concerns for lower-income students and families as they scrambled to upgrade internet service and procure enough devices for all of their children to attend school at the same time (Horowitz 2020). Few people would consider these things optional, or something that they could do without. Personally, avoiding interactions with Google would have been inconceivable during this same
period as my school email is a Gmail account. Beyond containing critical information from professors and administrators, checking my school email is codified in the student handbook. It is unavoidable. That makes it a very select few that have enough resources to sustain themselves without interacting with any surveillance capitalist derived services or products.

Furthermore, collective resistance to surveillance capitalism is prevented by its integration into daily life (Walker, Fleming & Berti 2021). When everything is connected to the internet, and through the internet to the surveillance capitalist establishment, then this level of observations and control can feed “inevitable” (Walker, Fleming & Berti 2021). As the platforms expand, incorporating school, leisure, and work and requiring individuals to mesh digital spaces with their lives, the scope and power of surveillance capitalism becomes overwhelming. Compounding this issue, the system feels arbitrary, controlled, and monitored almost completely by computer algorithms. It’s “government from a distance” (Walker, Fleming & Berti 2021, p. 38). With no human being to persuade or influence, surveillance capitalism feels even further removed and omnipresent. This erodes support for collective action because protest seems pointless and impossible. This is the attitude that a lot of people raised in the age of the internet hold. TikTok, infamous for its collection and sharing of PBD (Huddleston Jr. 2022, O’Flaherty 2021, Kelly 2022, Delfino & Johnson 2022), is the current social media app of choice and the host to content creators who constantly joke about how much information business and government has about them, with little anger or real fear (Brooks 2022). For people who have only known a world shaped by surveillance capitalism, and for a lot of others, these are simply the facts of life: dismal and upsetting but immutable. Accordingly, mobilizing enough people with enough resources to exit the surveillance capitalist sphere of influence would be incredibly difficult.
Also, users do not have a lot of bargaining power. In the current economic model of surveillance capitalism, users are laborers who provide a raw resource (PBD), which is then sold to their consumers, who are other companies. Resistance of a capitalist organization is most effective when a group has reciprocity with the company (Zuboff 2019b). Like with elected officials, the people ensuring your success (either through votes or through purchases) have the most impact. In this context, which would mean that the people purchasing PBD would have more impact than the people furnishing it. So, users have extremely limited bargaining power which would only be effective if they could adequately damage or interrupt the means of production.

Rebelling via boycott is, therefore, ineffective. Too many people are reliant on the services provided by surveillance firms to stop using them in defiance, too few people feel violated by this exchange and therefore motivated enough to make the necessary sacrifices. (Sevignani 2013). Organizing on such a scale would require many people to be very committed to a cause that might cost them in significant ways. They would have to pull their children from their education, risk workplace repercussions, lose contact with important family members, jeopardize friendships and relationships, and so on. Such a movement might stretch over an extended period, inducing further strain on protestors. And even if a large enough force could be organized, users are not in a strong bargaining position to begin with due to their position within the capitalist framework.

In a potential ideal scenario, business leaders are lobbied by concerned members of the public, change their ways and values and go about the process of change independently of exterior mandates and regulations. This is the goal of organizations like the Center for Human Technology, which focuses on “the insidious effects of persuasive technology [and] the runaway systems beneath” (Center for Humane Technology). Thus far they have been highly effective at raising the profile of their concerns about extractive technology through their educational resources (various TED Talks, The Social Dilemma on Netflix, and their podcast and activism). They argue that technology should be used for people, not for business; they argue for us to keep in mind the humanity of the people using the technology and internet currently dominating our world.
Additionally, collective action would assume that people are upset and feel as though their privacy must be protected. That is simply not the case and many feel as though "there [is] an actual, or at least a potential, informed consent by the user" to the gathering and use of personal behavioral data (Sevignani 2013). And those who are frustrated by the system of data gathering seem more concerned about the exploitative terms of their contract than the idea of surveillance (Sevignani 2013). There will be no organizing to protect people’s privacy if people do not feel like their privacy has been violated.

While this response aims to prevent the gathering of PBD, it does not make any provisions to prevent data from being made into a commodity, which is what makes the futures market possible. The collective action response most often focuses on the exploitation of workers in the gig economy and invasions of privacy, skipping over commodified personal data. Thus, even if it were to be successful, it would fail to prevent the commodification of PBD, which is the foundation step and surveillance capitalism and thus the critical juncture for the most effective intervention.

The Third-Party Intervention Approach

This approach is dependent on the flexibility of businesses and their willingness to adapt based on the wants and advocacy of interest groups. There is no assurance that businesses will want to take the high road, or that the arguments of activist organizations will be compelling enough for business leaders to change the foundations on which they have to build their revenue streams. Personal Data Spaces (PDSs) are a proposed solution that melds the interests of users

---

9 There is an argument to be made that the lack of frustration or issue with the current system is due to the opaqueness of the mechanics of surveillance capitalism. Information and education about surveillance capitalism is not readily available and additional transparency and education could potentially lead to more user motivated action. As discovered in this 2013 study by Sevignani, many users developed more negative perceptions of surveillance capitalist firms as they learned more about their business practices. This could translate into political action and a greater awareness of privacy issues.
and businesses. They “promise users a place in the driver’s seat for the use of their personal
data” (Lehtiniemi 2017). Personal Data Spaces would be 3rd party platforms that host personal info banks and facilitate the exchange of PBD. Businesses could request access to these info banks in exchange for a fee, or more likely for access to their company’s services. It aims to eliminate some of the vulnerability, information inequity, and power asymmetries that are inherent in the current data extraction logic. While potentially leading to “intensify[ing] datafication,” they also aim to ensure that individuals have much more control over who is looking at their information and how it is used by coordinating negotiations and fair contracts between users and extractors (Lehtiniemi 2017). PDSs intervene at the point of exchange in the hopes of making it more equal and ensuring better benefits for data sources.

This solution requires extensive new digital infrastructure. It cannot prevent companies from gathering data when you use their sites, meaning that users would have to use specialty email addresses, search engines, and ad blockers, and be incredibly careful about their cookie permissions among other things (Lehtiniemi 2017). Data would have to be uploaded to cloud-hosted info banks on a third-party service, which is an additional barrier to entry. Then, the user would have to have data that was worth enough that companies would be willing to pay, or trade services, for access to it. Contracts would have to be signed and approved, meaning legal teams for potentially both parties. Surveillance capitalism relies on big data, massive amounts of information synthesized and analyzed until it is useful to them. As a result, “our ‘personal’ data only becomes meaningful—and gains value—as a commodity at scale (Malmgren 2019). This means, should PDSs become a norm, Surveillance capitalism's free raw resources could quickly become incredibly expensive. It also means that these firms would have to start thinking about data differently: in terms of what we know about a person, as opposed to the amorphic abstract
web of data insights that they currently use (Bottis & Bouchagair 2018). This could be a win for the user, but the risk of this means there would be staunch opposition from businesses to this shift.

However, there are other concerns from a user standpoint. The foundational idea of PDSs is that users have more autonomy over their data and digital footprint because they get to be active participants in the exchange of data, determining who and when, and how, thus empowering them. This is dependent on fair and non-exploitative contracts. As noted previously, the current system creates and sustains substantial power asymmetries, meaning that in this scenario the user does not necessarily have bargaining power. If a user is negotiating with Google, for example, they would need to be able to walk away from the table. Right now, that is not always possible. Surveillance capitalist firms provide integral services to users for their work, essential communication, and even their leisure. That means that they hold all the power here. If they ask someone to divulge more data than an individual might be comfortable with, then most consumers will be forced to swallow their discomfort and share that data. Thus, PDSs might exacerbate the problem, and remove the peaceful benefit of ignorance. And they might be an expensive service for users. If someone cannot afford to let PDSs help you regulate your data, are they then not afforded the same level of data privacy as their richer counterparts. In such a setup, privacy could only be ensured with wealth, leaving poorer people out in the cold: heavily surveilled and the vulnerable. PDSs profoundly fail to reduce or prevent the commodification of personal behavioral data; instead, they work within the confines of surveillance capitalism in the hopes of protecting the most vulnerable parties in these exchanges. It is a valiant attempt, but one that falls short of its goals in many ways.
The Governmental Approach

This leaves government regulation as a final potential approach, with all the complications that that entails. Government regulation supersedes the wants and goals of business without jeopardizing the lives and livelihoods of users. It exists exteriorly from the market and is thus not subject to the limitations of market pressures. So, government can sidestep many of the barriers to enacting effective shifts in the surveillance capitalist industry. Countless countermeasures have been proposed, from subjecting PBD to trade secret rules (for which there is considerable precedent as algorithms are considered trade secrets) to protecting them via property rights (and making a privacy argument for property rights) (Bottis & Bouchagiar 2018, Prins 2006, Malgieri & Custers 2018).

At first glance, it seems like a silver bullet in the war against the commodification of personal behavioral data. However, as illustrated in earlier sections of this paper, the commodification of PBD lies at the heart of this issue, and many if not most of these solutions rely on codifying this commodification. Trade secrets are protected under intellectual property laws; they are “a complement to patent protection” (United States Patent and Trademark Office 2022). The Defend Trade Secrets Act of 2016 and the original Economic Espionage Act of 1996 allowed for the litigation of these cases which can result in the seizure of trade secrets and the organization being compensated for their loss (Defend Trade Secrets Act of 2016). Even the language ("seizure") mirrors that of personal property laws, which have also been proposed as a way to target invasions of privacy. Under either of these approaches, we would have to consider the personal behavior of a person to be their personal property. In its most traditional form, property is "a general term for the rules that govern people's access to and control of things like land, natural resources, the means of production, manufactured goods" (Waldron 2020). A
person possesses these rights to access or control an object, owns it. Ownership can transfer, meaning that these things can be traded. Thinking about a person's personal behavioral data as something that an individual owns, therefore, also implies that it is a concrete, bounded thing that is capable of being exchanged, a bit like a commodity. Thus, it is possible to claim that by protecting privacy as if it were the personal property of the individual, the law would be creating a legal foundation and precedent for commodification.

We have seen measures be effective in limiting the impacts of surveillance capitalist business models in the EU, with their General Data Protection Regulation, or GDPR. The act protects citizens on the EU and all the internet traffic in EU territories. It fines companies found in violation of its principles, which are “lawfulness, fairness and transparency; purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability” (Wolford). More concretely, The GDPR forces companies to responsibly harvest, store, and use data and it created more control mechanisms for users. In this act, finally fully established in 2018, the EU created firm limits on how corporations can use PBD and strong reinforcements of individual privacy rights (Aho & Duffeild 2020). The act was designed to target the nudging activity that so concerns many people doing work on this subject and aimed to be "profoundly socially grounded" (Syroundis et al.). The motto of the act and the associated regulatory agency is "data protection by design and by default" (Syroundis et al.). Though the act promises massive sanctions, it seems to have only been moderately effective in enforcement (Syroundis et al.; Kollnig et al). According to some advocates, "We have failed to realize the potential of G.D.P.R. thus far" (Satariano 2020). But it has caused some frustration on the part of tech companies, with Meta repeatedly threatening to pull Facebook from Europe should the region fail to make their preferred accommodations (Deutsch and Bodoni 2022). This piece of
regulation is far from perfect, but we have seen it become a larger and larger presence in global economic policy, and it may be a step in the right direction. It is one of the few proposed responses that would target the gathering of PBD, not the side effects of doing so.

Of course, there are some concerns about trusting the government to regulate tech companies’ surveillance. In the US, the Patriot Act and subsequent increase in governmental surveillance have been aided by surveillance capitalism. As early as 2004 the CIA contracted Google to share information that might be relevant to their investigations (Zuboff 2019a). Government regulation is reliant on the government wanting to regulate, meaning that they have to think that surveillance capitalism is doing something wrong: that PBD is private, and that privacy is worth protecting. In the US, the history of privacy protections has been limited to medical contexts, the intimacy of marriages, and sexuality of individuals, which could pose an issue to the following policy proposals that would expand the boundaries of the definition.

Government regulation might also look like it does in China, where surveillance capitalism has been harnessed to help create their Social Credit System (SCS) to help bridge their bureaucratic gaps, thus further constraining choices and behavior through state sponsored surveillance and monitoring (Aho & Duffield 2020). It’s a mixed bag.

However, government policies remain the best option. In a perfect capitalist system, the market would regulate itself. But, without exit options or a capitalist establishment responsive to user demands, this is not feasible because “‘user’ dependency is the fulcrum of the surveillance capitalist project” (Zuboff 2019b p. 21). Individuals are unable to bring about change in business because they do not have enough bargaining power to make an impact on their profit margins or to reliably prevent companies from gathering their data. Third parties fail to do anything more than offer band aid solutions and attempt to return some autonomy and control in how data is
used. However, none of these genres of response address commodification and some, like a few governmental interventions, actively substantiate and codify the process. Thus, effective responses to commodification, and through it surveillance capitalism, will have to come from advocate governments who can operate outside of the system and work to reform it.

**Policy Proposals**

I propose the government separates profit from data gathering. This proposal leans on the legal tradition of securities trading regulations. The Advisers Act of 1940 attempted to eliminate conflict of interest of financial advisors when providing recommendations and their clients, as related to the advisors’ own stake in the stock market. At a time, Congress wanted to mitigate the influence that investment and financial advisers could have on the market through securities trading, since they were in a position to affect its outcomes for their own self-interest (U.S. Securities and Exchange Commission 2013). The law, amended in 1996 and in 2010, required that most investment advisors register with either state regulatory agencies or the federal regulatory agency, the Securities Exchange Commission (SEC). This registration allowed for the government to monitor advisors, which is a cautionary and limiting factor on the advisor's ability to give recommendations which may have positive personal ramifications. Explicitly, it prevents advisors from profiting from the advice they provide to clients. Though the act has significant shortcomings and loopholes (Tittsworth 2013), it is a major focus of the SEC. Earlier this year, following a string of updates, they announced yet more plans for additional rules under the Advisers Act that would target investment advisors, forcing them to provide more comprehensive documentation of their activity, and increase protections for private fund investors (Anderson et al. 2019, SEC 2022).
The purpose of the Advisers Act is to prevent individuals from benefiting from an information asymmetry, a term popularized by economics which refers to a phenomenon where an organization or entity holds either superior or more information than their counterpart. This allows the first party to maintain power and subordinate the second party. Lightfoot and Wisenieeski (2014) provide the historical example to illustrate. Referring to the Middle Ages, “clergy not only monopolized writing and literacy but also were able to define what was legitimate thought and what was heresy,” thus giving the Church tools to control populations, and punish them for disobedience (p. 215). In the case of investment advisors, the subordination is less apparent or dramatic, but it is still possible for them to engage in asymmetrification, or “the deliberate withholding and manipulation of the knowledge” (Lightfoot & Wisenieeski 2014, p. 214). Advisors are in a unique position to spin the recommendations they provide to clients in such a way that the advisors’ investments benefit because of the actions of the client. Advisors know what a client will do and can make adjustments to their investment portfolio to benefit from it. Or, even worse, they can steer a client in a particular direction because of how it might benefit their portfolio. It has similar hallmarks to insider trading.

The misuse of information, and access to the decision making of others, is problematic for an ideal market, which is supposed to fluctuate based on the response of consumers, not the interests of securities traders. Concern over this prompted Congressional action and the passage of the Advisers Act.

I move for a similar response to the commodification of personal behavioral data and surveillance capitalism. Though the securities market and the futures market are not completely analogous, there are significant crossovers in the production of information asymmetries and those with access to information benefitting unethically. What the Advisers Act does is separate
opportunities to make profit from information gathering. Though a much more complicated logistical question on the part of surveillance capitalism, similar measures could prevent companies from selling the predictions created from PBD, thus making PBD valuable, not as a commodity, but as information. Companies could still use their metrics to improve their services, understand their internet traffic, and monitor consumer interactions, but they would not be able to use this data to inform their advertisement work or to share their analysis of user data with other companies who would use that to sell goods or service. The two parts of the business would have to become separate enterprises.

In this case, we would not be preventing data gathering. Data exhaust is unavoidable and the tools for surveillance readily available, resulting in a lot of difficulty in simply halting the process. This does not eliminate concerns over exploitive contracts or ‘terms and conditions., lack of transparency in how data is gathered, or general attitudes within the field about user privacy. The hope is that by separating profit-making and surveillance, government can interrupt the process of commodification by interrupting the production of futures markets. Companies are not able to use their platforms to gather information that they can then use to increase their profitability by manipulating and constraining the behavior of consumers. The primary focus of this paper was to investigate the harms of commodification which have been under discussed and realized and explore potential responses. Though this separation does not solve all the issues inherent to surveillance capitalism, it does target the initial step in the process, thus establishing some essential protections for users.

Conclusion

The issues and concerns associated with surveillance capitalism are broad and wide-reaching. Surveillance capitalism has influence in countless fields of study and parts of life, and
that makes it incredibly threatening. It can seem all powerful, all knowing, and omnipresent. This research does not attempt to diminish the fear and worry associated with this system. Instead, it hopes to shift our focus and our aims. Concentrating our efforts on the symptoms of surveillance capitalism will not be effective. These are band-aid solutions for a root dysfunction that is manifesting as, or facilitating, breaches in choice autonomy, privacy, and labor protections. The foundational issue, I argue, can be linked to the idea that human beings' personal interests, behavior, and interactions, are sellable. The paper has outlined the issues and harms associated with this assumption, but I would like to reiterate what I consider to be the largest problem here: that it creates a futures market where predictions, created via gross violations of privacy, are worth more if they are accurate, which instigates attempts at behavioral modification. Without attacking the commodification of personal behavioral data, this market endures, and the larger system will simply be monitored or marginally regulated and will sustain no lasting impacts.

It is worth doing. Beyond the philosophical or ethical concerns that I just discuss, this has significant tangible impacts on how we lead our lives. For some, it is a matter of exposure to other ways of thinking which is confounded by their careful confinement in a filter bubble. For others, it is a matter of physical safety, as their data is publicly available to anyone with a credit card. Capitalism has always been inherently predatory and exploitative. Surveillance capitalism does the same things, but it uses our own behavior against us. The stakes are too high to allow companies with little to no interest in the wellbeing of users, who they see as a resource, to make money selling information that they stole in the first place.
Works Cited:


https://doi.org/10.1080/03085147.2019.1690275


American Booksellers Association Advocacy Division (2021). *American monopoly: Amazon’s anti-competitive behavior is in violation of antitrust laws.*

https://www.bookweb.org/sites/default/files/diy/American%20Booksellers%20Association%202020%20Amazon%20White%20Paper_0.pdf


https://doi.org/10.1016/j.cie.2019.106099

http://dx.doi.org/10.2139/ssrn.3313837


https://doi.org/10.4236/ojpp.2018.83015


Brooks, Griffin Maxwell [GMB] (2022). “*Look, I know that targeted advertising is bad...*”

[Video] TikTok. https://www.tiktok.com/@griffinmaxwellbrooks/video/7090181736189037970?_t=8RzTPOig2zj& _r=1 GM

Challener Jr., W. A. (1949, Fall). The doctor-patient relationship and the right to privacy.

*University of Pittsburg Law Review*. https://heinonline-org.ezproxy2.library.arizona.edu/HOL/Page?collection=journals&handle=hein.journals/u pitt11&id=630&men_tab=srchresults#


https://plato.stanford.edu/cgi-bin/encyclopedia/archinfo.cgi?entry=privacy


Huddleston Jr. T. (2022, February 08). *TikTok shares your data more than any other social media app — and it’s unclear where it goes, study says.* CNBC. https://www.cnbc.com/2022/02/08/tiktok-shares-your-data-more-than-any-other-social-media-app-


https://www.washingtonpost.com/technology/2022/01/24/tiktok-privacy-settings/


Madrigal, A. C. (2012, March 01). Reading the privacy policies you encounter in a year would take 76 work days. The Atlantic.
https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/


https://ebookcentral.proquest.com/lib/uaz/detail.action?docID=683949&pqorigsite=primo


Wolford, B. *What is GDPR, the EU’s new data protection law?* GDPR.eu. https://gdpr.eu/what-is-gdpr/

