Non-domination as a barely fulfillable aspiration under surveillance capitalism: A republican perspective at the individual level

Helder, Micha

Non-domination as a barely fulfillable aspiration under surveillance capitalism

A republican perspective at the individual level

Master Thesis

18th of December 2025

Student: Micha Helder

Student number: S1706780

Program: Master Philosophy (60EC)

Specialization: Philosophical Perspectives on Politics and the Economy

University: Leiden University

Supervisor: Prof. dr. D.M. Mokrosinska

Special thanks to my father and my girlfriend

Table of Contents

Abstract

Surveillance capitalism has become a dominant business model in contemporary digital economies, and it is characterized by the large-scale collection, processing, and commercialization of personal data. This thesis responds to the work of Benn and Lazar (2021), who argued that surveillance capitalism, although harmful at a societal level, can hardly be shown to do moral harm on the individual level. Building on their conceptual framework that investigates the impact of surveillance capitalism-based practices at the societal level on three domains, privacy, exploitation and manipulation, this thesis examines the consequences of paying for virtually indispensable services with personal data at the level of the individual. This thesis re-evaluates whether the renouncement of personal data might put individuals at risk of moral harm by the power exercised by surveillance-capitalist entities. Grounding the analysis in a neo-republican framework (Pettit 2016), this thesis argues that pervasive data collection and inference practices expose individuals to standing vulnerability due to privacy loss. It further contends that structural power asymmetries and the absence of meaningful alternatives amount to domination through the lens of exploitation. Finally, while direct manipulation cannot be shown to amount to domination on the individual level, algorithmic control over informational environments enables forms of indirect manipulation that undermine individual agency. In contrast to Benn and Lazar (2021), the thesis concludes that surveillance capitalism-based practices pose a serious threat to individual freedom as non-domination.

1 Introduction

Surveillance capitalism is a recent and rapidly expanding mode of economic organization, characterized by the collection, analysis, and commodification of personal data by corporate actors. At its core, this system relies on gathering detailed information about user behavior with the aim of predicting and if possible shaping future actions, in most cases ultimately to sell personalized advertisements. Many people, including myself, experience an uneasy sense of being constantly monitored and potentially manipulated in nearly every interaction with internet-connected technologies. It should be realized that 'free internet services' exemplified here by efficient and user-friendly internet browsers such as Google Chrome (Alphabet), Microsoft Edge (Microsoft) and Safari (Apple), and searching machines such as Google (Alphabet), Bing (Microsoft) and Yahoo! (Microsoft) can't be truly free, in the sense that someone needs to pay for their development and maintenance somehow, and the businesses operating these services are no less motivated to make profit than any other business. In contrast to most services that we are used to – being services paid for by a monetary transaction – the afore mentioned services are effectively paid for with a new type of currency. 'Personal data' is the nature of this currency, which could be considered as a non-explicit currency. This non-transparent payment model may or may not constitute a fair business practice. Yet a feeling of eeriness remains once an individual realizes the consequences of this relatively new and poorly tangible business model. This thesis stems from that intuitive sense of discomfort and asks whether it can be normatively substantiated: can we show that surveillance capitalism, as a system, inflicts moral harm on individuals by gathering and using their data?

To investigate this question, I will draw on the framework of republican political philosophy as developed by Philip Pettit. Republicanism, in this modern formulation, departs from the classical liberal emphasis on freedom as non-interference. Instead, it defines liberty as *non-domination*, that is, the condition in which no actor holds arbitrary power over another, regardless of whether that power is exercised. I do not wish to engage in arguments for or against republicanism, and neither do I want to engage in a defense of why this particular version of the theory should be preferred over others. For the sake of consistency, I must settle on a single interpretation of Republicanism, and I have chosen the theory as argued for by Philip Pettit in a leading article entitled "*A Brief History of Liberty – And Its Lessons"* (2016). In this article Pettit gives a synopsis of the history of Republicanism and contrasts it with Liberalism. I will briefly go over both what he refers to as *classical republicanism* and modern *neo-republicanism.* Classical republicanism is the republican theory as forwarded by ancient authors (see below), and neo-republicanism – henceforth simply referred to as *republicanism* – is the theory that Pettit himself argues for.

Pettit traces the roots of republicanism to classical Roman thought, particularly in the writings of Polybius (≈203 – 120 BC) and Cicero (106 – 43 BC) and identifies three interlocking commitments that characterize the tradition: (1) freedom as non-domination, that is the absence of actors capable of arbitrarily interfering in one's life (Pettit 2016, pp. 6-7). Domination could occur both by the state as *public domination* and from non-state actors as *private domination,* (2) a mixed constitution in which political power is shared among different bodies, so that

power is limited through institutional checks and balances, and (3) a contestatory citizenry willing and capable of resisting both private and public domination. Freedom for the individual, in this view, is when no other actor holds the power to arbitrarily interfere in their life. As such, it is not a matter not being interfered with as it is in liberal terms, but of living under relations of mutual accountability where no one can look down on another with reason for fear or deference – the so-called "eyeball test" (Pettit 2016, p. 9). This conception of liberty recurred in the Renaissance animated early modern revolutions and continues to inform neo-republican critiques of contemporary power structures. Pettit contrasts this lineage with liberalism, which understands freedom primarily in terms of non-interference, and argues that a republican perspective offers a more robust account of what it means to be free in a world structured by institutional and systemic power.

To assess whether surveillance capitalism is morally objectionable in republican terms, it is first necessary to clarify what the practice entails. For this purpose, this thesis primarily relies on Shoshana Zuboff's analysis in *The Age of Surveillance Capitalism* (2019). Zuboff defines surveillance capitalism as "*a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales*" (p. 9). Reformulated, it is a business model centered on the large-scale collection of behavioral data from users of digital services, which are then processed by algorithms to construct detailed individual profiles. These profiles are used not only to predict future behavior but increasingly to influence and steer it – thus integrating surveillance and behavioral manipulation directly into the logic of profit-making. In this system, private entities that can predict and shape user behavior most accurately gain a competitive advantage by selling higher-priced, more effective advertisements.

Before moving on to defining the main research question I hope to answer in this thesis, I will briefly go over the main differences between surveillance capitalism and 'regular' capitalism. Apart from individuals *de facto* paying by allowing the collection of their data instead of paying with regular currency, surveillance capitalism distinguishes itself from earlier forms of capitalism is not simply by its technological sophistication, but by its departure from prior norms of reciprocity, transparency, and public anchoring. In Chapter 18 of her book (pp. 309–19), Zuboff highlights three structural innovations that set surveillance capitalism apart: the erosion of the traditional balance between knowledge and freedom, the breakdown of reciprocity between corporations and users, and a stance of radical indifference toward societal values. First, where classical capitalism presupposed imperfect knowledge on all sides of the market, surveillance capitalism breaks this symmetry by granting dominant firms unprecedented insight into individual behavior – often more than individuals possess about themselves. Second, while earlier capitalist enterprises relied on valuing individuals as both employees and consumers, surveillance capitalism treats them primarily as sources of data and targets for advertisements. Third, it is fundamentally indifferent to the political and moral implications of its operations. Its primary concern is maximizing data extraction and user engagement; concerns such as truth, democratic integrity, and social cohesion are externalities, not corporate priorities.

These features raise important normative questions about the kind of power surveillance capitalism exerts over individuals. The platforms at the heart of this model offer environments that resemble extensions of the public sphere – spaces where people interact, exchange ideas, and form relationships. Yet these environments are largely privately owned and governed, lacking the transparency and accountability that would be expected if they would have been public institutions. There are a few exceptions such as the internet browser Firefox (subsidiary of the non-profit Mozilla Foundation) and Signal (developed and owned by the Signal Foundation, a non-profit organization). With 2,57% market share for internet browsers (StatCounter GlobalStats 2025), and with 70 million Signal (Business of Apps 2025) users these alternative platforms constitute a small minority. Hence, it can be said that surveillance capitalism-based companies such as Alphabet, Microsoft and Apple create a form of *private domination* over users, whose behavior is monitored, analyzed, and nudged in ways that users do not fully understand and cannot meaningfully contest.

Accordingly, this thesis is guided by the following central question:

To what extent can the corporate practices of surveillance capitalism be shown to interfere with individual freedom when analyzed through the republican concept of non-domination?

To address this question, this thesis examines three domains in which surveillance-capitalist practices may undermine individual freedom: *privacy*, *exploitation*, and *manipulation* (Benn and Lazar, 2021). I begin by establishing a working account of freedom as non-domination, after which I provide a motivated overview of these three potential forms of harm. The subsequent chapters evaluate each domain in turn, analyzing whether the mechanisms involved plausibly constitute forms of domination at the level of individual users. This analysis is organized around the following sub-questions:

1. *Does the loss of privacy associated with the use of surveillance-capitalist platforms expose individuals to forms of domination?*
2. *Do the economic relations between users and surveillance-capitalist firms amount to exploitation in a way that constitutes domination?*
3. *Do the manipulative techniques employed by surveillance-capitalist systems interfere with individuals' agency such that they become vulnerable to domination?*

By assessing each of these potential harms through the lens of non-domination, this thesis aims to clarify whether, and if so, how surveillance capitalism poses a significant threat to individual freedom. The conclusion will be that insofar as individuals are reliant on the services and platforms of surveillance capitalist firms, they are subjected to the arbitrary power of corporate actors and hence compromised in their freedom as non-domination.

2 Freedom as non-domination

In this chapter I will give a working definition of freedom as non-domination. I hope to formulate a definition that can be referenced throughout the remainder of this thesis. Furthermore, my definition is aimed at providing clear requirements which must be met for freedom as non-domination to obtain.

In Pettit's republican account (2016, pp. 15-17), freedom as non-domination is a conception of liberty according to which an individual is free only insofar as they are not subject to the *arbitrary power* of others. Whereas the liberal view of freedom as non-interference defines liberty in terms of the absence of direct obstacles or coercion (Mill 2011), non-domination focuses instead on the structural condition of power relations. A person can be dominated even if they are not actively interfered with, so long as another actor holds the unchecked capacity to intervene in their choices.

An example of domination would be the relation between a master and a slave in ancient Rome. Supposing for the sake of argument that the master has a benevolent character and never harms the slave in any way, the slave would still be dominated by the master. Even if the slave can do whatever they would want without the master obstructing or threatening to obstruct them in any way at all, at any given point in time the master *could* theoretically interfere in the life of the slave. In ancient Rome slaves were the property of their masters, so the master in this example has the option to do whatever they would please to the slave if they desired. Our master is benevolent so never acts upon this option, but the mere possibility of arbitrary interference is enough in a republican account of freedom to consider the slave to be dominated and hence unfree (Pettit 2016, pp. 5-7, McCammon 2018).

Crucial to the definition of domination is the notion of *arbitrariness*: power is arbitrary when it can be exercised without being constrained by contestable rules, norms, or procedures that serve the interests of those affected (Pettit 2016, p. 16). In contrast, non-arbitrary power is bound by laws, institutions, or practices that are contestable and accountable to the people subject to them. Thus, to enjoy freedom as non-domination is to live in a condition where others cannot impose their will unchecked, but where the use of power is systematically restrained so that individuals stand as equals, protected against domination.

More formally defined, the power to intervene is arbitrary if:

1. The interests of the affected party are not being served by the interfering party
2. The affected party cannot contest the interference
3. The affected party cannot hold the interfering party accountable for their actions

For there to be the possibility of arbitrary interference, only one of these conditions needs to be met. In other words, the possibility for interference is not arbitrary only if the interference serves the interests of the affected party, the affected party can contest the interference, and the affected party can hold the interfering party accountable for their actions.

If we apply these rules to the example of the master and slave in ancient Rome, it becomes apparent that the slave is unfree. Although the master clearly takes the interests of the slave

into account, the slave can neither contest any interference in their life by the master, nor can the slave hold the master accountable for any of their actions.

In the following chapters I hope to use this definition to be able to clearly determine whether any possibility to interfere in the life of individuals by surveillance capitalist actors is arbitrary or not, and hence whether it could be considered as domination.

2.1 Formal definitions

I would like to provide some more formal definitions as well to clearly delineate what I take the core concepts in this thesis to mean. For each of the concepts below I will also have a short explanation of the concept.

In subsequent chapters I will introduce three more concepts of which I will provide formal definitions in the same style.

Formal definitions, in which:

- A = individual
- B = corporate actor
- *P* = what A wants to do
- *Q* = what B wants A to do
- *P* is not *Q*

(straight capital: actors, capital in italics: intended actions)

Non-interference

- A wants to do *P*
- B wants A to do *Q*
- B does not make A do *Q*
- A does *P*

For non-interference to occur it is inconsequential whether B had the ability or desire to make A do *Q* instead of *P*. In this case B simply doesn't make A do *Q*. Non-interference as such is what would capture liberal freedom, in which A is free as long as A is not interfered with.

Interference

- A wants to do *P*
- B wants A to do *Q*
- B makes A do *Q*

When interference occurs, it is taken for granted that B was able to make A do *Q* instead of *P*. I take interference in this sense to capture non-freedom in liberal terms.

Non-domination

- A wants to do *P*

- B wants A to do *Q*
- B cannot *arbitrarily* make A do *Q*
- A does *P*

Non-domination occurs when B cannot make A do *Q* instead of *P arbitrarily*. I am leaving the exact reasons as to why B would be unable to make A do *Q* to make the definition as all-encompassing as possible. Non-domination captures republican freedom if there is no possible B that can interfere with A *arbitrarily*. I have worked out the details of arbitrariness above in the section on Freedom as non-domination.

Domination

- A wants to do *P*
- B wants A to do *Q*
- B can *arbitrarily* make A do *Q*

Domination happens when B can *arbitrarily* make A do *Q*. Whether B acts on this possibility or not is of no consequence for domination to occur. Domination is equivalent to the absence of freedom on Republican terms.

With these more formal definitions I hope to be able to clearly evaluate possible occurrences of domination of individuals by surveillance capitalism. Before doing that, I will proceed to delineate the areas in which individuals can be dominated by surveillance capitalist firms.

3 Areas of wrongdoing

In this chapter, I will provide an overview of the key areas in which surveillance capitalism may harm individuals. This chapter draws on the work of Benn and Lazar (2021), who identify three main forms of wrongdoing associated with surveillance capitalism (or automated influence, as they themselves term it): *privacy*, *exploitation*, and *manipulation*. In their paper, Benn and Lazar (2021) argue that the strongest case against the practices of surveillance capitalism can be made by examining its structural or collective effects, rather than focusing on the individual level.

My research will focus on these same three areas but with a crucial difference: I will explicitly investigate the possibility of wrongdoing against individuals. Furthermore, in contrast to Benn and Lazar (2021) I will base all my arguments on a single theoretical framework – republicanism – as outlined in the section above. The following section will provide an overview of each of the three areas of wrongdoing and outline their main sources as identified by Benn and Lazar (2021). I will present them in their original order and will use this same order throughout this thesis for the sake of consistency.

3.1 Privacy

Benn and Lazar (2021) argue that individual privacy has been violated by surveillance capitalism on such a vast scale and with such depth that there is little doubt these violations are occurring, and that they are "obviously wrong" (p. 129). At the individual level, Benn and Lazar contend that claims of ownership over personal data are problematic, as data is rarely exclusively about a single person. Much of the sensitive knowledge that surveillance capitalists possess is generated by combining numerous data points, a practice that is not clearly morally impermissible.

Furthermore, Benn and Lazar (2021) argue that the notion of meaningful consent to surveillance is flawed. While they acknowledge that, at an individual level, "the only meaningful choice is between not using the internet at all and submitting to being profiled and targeted" (p. 131), they contend that a solution must come from a collective commitment to valuing privacy as a society, given the consequences that the erosion of privacy has for society as a whole. They conclude their section on privacy by warning that surveillance capitalism and the technologies that support it allow a small number of actors to accumulate an excessive concentration of power, through the sheer volume of knowledge they control. This threatens both freedom and equality at the societal level (p. 134).

3.2 Exploitation

Benn and Lazar (2021) define exploitation as a situation in which one party in a seemingly voluntary exchange takes advantage of significant asymmetries of knowledge, power, and/or resources - an exchange the other party would not have agreed to if not for this imbalance (p. 135). They begin their section on exploitation by noting that complaints of individual-level exploitation by surveillance capitalism (or “influencers” as they term them) are rarely heard. While there is an undeniable asymmetry in knowledge, power, and resources between

individual users and major tech platforms, the exchange may still appear fair: individuals benefit from using these platforms, while the data they provide may seem trivial or worthless to them.

However, on a broader scale, if large numbers of individuals make a similar decision, namely trading their data for access to "free" platforms, the case for exploitation becomes more convincing. Not only do corporations gain extensive data on individuals, but by aggregating and processing this data, they acquire far greater knowledge and power over society as a whole. This surplus of knowledge and power, generated from the data of many individuals, is something no individual alone can claim, but Benn and Lazar argue that we, as a self-governing society, can (2021, p. 138).

3.3 Manipulation

Benn and Lazar (2021) acknowledge that attempts to manipulate individuals by data-driven commercial entities occur on a large scale, with varying degrees of success. They argue that although some individuals may genuinely feel manipulated by surveillance capitalists, for most people, these practices amount to little more than subtle nudging. However, on a societal level, even subtle nudging that occasionally persuades individuals to take specific actions or purchase certain products can have far-reaching consequences. The following quote encapsulates their main reason for constructing arguments about manipulation at the collective level:

> "*The central moral concern of stochastic manipulation is less its effect on individuals whose decisions are swayed, and more that these new techniques enable small groups of savvy people to exercise a disturbing amount of power over groups and populations at large*" (Benn and Lazar 2021, p. 142).

In the next sections I will focus on these same areas in turn, rather looking at the individual than at the societal level, and evaluate the possible harms of surveillance capitalism to individuals through a republican lens. In Intermezzo 1 use an excerpt of the Google Privacy Policy conditions to show the kind of (intimate) data that Google is allowed to collect once an individual has accepted the general conditions.

Intermezzo 1

The following excerpt shows the kind of information that Google collects from its individual users. By accepting the general Google terms and conditions, the individual gives consent that the following types of data are collected, furthermore, Google lists how such data is collected. Italics by author of this thesis (Google 2025).

"Your activity: We collect information about your activity in our services, which we use to do things like recommend a YouTube video you might like. The activity information we collect may include: Terms you search for , videos you watch, views and *interactions* with content and ads, v*oice and audio information*, purchase activity, *people with whom you communicate or share content*, activity on third-party sites and apps that use our services , Chrome browsing history you've synced with your Google Account, *location data,* which includes GPS and other sensor data from device (such as an accelerometer or gyroscope), IP address and where you are active on Google services, and *information about things near your device*, such as Wi-Fi access points, cell towers and Bluetooth-enabled devices.

We may also *collect information about you from trusted partners*, such as directory services who provide us with business information to be displayed on Google's services, marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from partners to provide advertising and research services on their behalf.

We use various technologies to collect and store information, including cookies, *pixel tags*, local storage, such as browser web storage or application data caches, databases, and server logs. A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is opened.

If you use our services to make and receive calls or send and receive messages, *we may collect call and message log information like your phone number, calling-party number, receiving-party number, forwarding numbers, sender and recipient email address, time and date of calls and messages, duration of calls, routing information, and types and volumes of calls and messages.*"

4 Privacy

The aim of this chapter is to provide an answer to the question:

Does individual privacy loss occur when they engage with the platforms of surveillance capitalist firms in a way that amounts to domination?

To answer this question, I have divided this chapter into four sub-sections: Firstly, I would like to give a working definition of privacy for the purposes of the current thesis. Secondly, I would like to show both how a significant loss of individual privacy occurs due to the practices of surveillance and how this process can be considered a form of domination of individuals by corporate actors. Thirdly, I would like to evaluate whether this loss of privacy affects individuals in a way that can be considered a form of domination. Fourthly, I would like to argue that privacy can be an effective shield against other forms of domination such as laid out in the chapters below on exploitation and manipulation. Conversely, the loss of privacy that individuals experience when making use of the platforms and services of surveillance capitalists puts the individuals at greater risk of such other forms of domination.

4.1 Defining privacy

Formal definition:

- A wants to do *P*
- B wants A to do *Q*
- B lacks relevant knowledge about A such that B cannot make A do *Q*
- A does *P*

I take privacy to be a condition which can be enjoyed by individual actors. This condition is one which the individual both has control over which other actors gain access to data about them and can limit the ability of other actors to create new data about them. Privacy as such is not a binary condition, rather it is a spectrum that indicates the degree to which an individual actor can be said to enjoy privacy.

In relation to surveillance capitalism, I take privacy to be a condition which if enjoyed secures for any given individual the absence of being tracked, recorded or monitored in any way when engaging with online services. Privacy could be seen as the ability to act without any other actor registering, processing and saving data about one's actions.

Central to the business of surveillance capitalism the algorithmic gathering and processing of data about nearly everyone. Before being able to give any answer to the question of whether this loss of privacy constitutes a form of domination and as such leads to a loss of freedom for individuals, I would like to examine the process by which individuals come to at least legally agree to their loss of privacy and the surrender of the ownership of their data to corporate actors.

4.2 The process by which users lose the right to their data

Users of 'free' digital services routinely must accept *Terms of Service* or *Privacy Policy* agreements, thereby granting companies the right to collect and use their data. If any regular

internet user were to read all the privacy policies they encounter, a 2008 research paper estimated an approximate time-investment needed of 201 hours per year. If all American were to do so, they calculated the value of the national time lost at some 781 billion US$ annually (McDonald and Cranor, 2008, p. 565, via Zuboff, 2019, p. 39). In effect, individual users sign away any legal claim to the information generated through their online activities. Yet the implications of these agreements are often obscured by vague, technical, and inaccessible language. To quote:

> *"Legal experts call these "contracts of adhesion" because they impose take-it-or-leave-it conditions on users that stick to them whether they like it or not. Online "contracts" such as terms-of-service or terms-of-use agreements are also referred to as "click-wrap" because, as a great deal of research shows, most people get wrapped in these oppressive contract terms by simply clicking on the box that says "I agree" without ever reading the agreement. In many cases, simply browsing a website obligates you to its terms-of-service agreement even if you don't know it. Scholars point out that these digital documents are excessively long and complex in part to discourage users from actually reading the terms, safe in the knowledge that most courts have upheld the legitimacy of click-wrap agreements despite the obvious lack of meaningful consent"* (Zuboff 2019, pp 38-39).

Services are marketed as "free," concealing the fact that, as Stahl notes, "*their data is the* quid pro quo *for the use of the service and that the service is only available to them conditional on their making their data available and accepting the terms of service*" (Stahl 2023, p. 43).

Even when users attempt to protect their privacy, their options are limited. Configuring the most restrictive privacy settings is both tedious and only marginally effective. As Benn and Lazar (2021) observe, "*the only meaningful choice is between not using the internet at all and submitting to being profiled and targeted*" (p. 131). Moreover, personal efforts at privacy might be undermined by the behavior of others. As Véliz (2021) explains, if those around you share sufficient data, almost as much can be inferred about you as if you had never tried to protect your privacy at all (pp. 88–96).

There is a structural imbalance at play between the individual users who want to use the internet and make use of "free" services, and the surveillance capitalist companies that give the user no choice but to accept their *terms of service*. The asymmetry of power between vast corporate entities and individual users is profound. Individuals who wish to engage online – whether in their private or professional life – are faced with an illusory choice: either accept the terms imposed by surveillance-capitalist firms or to be effectively excluded from participation. I would like to draw attention especially to the fact that individuals effectively lose freedom in this process. Individuals have *no choice* but to accept the terms of service, which I would argue are not in favor of the individual on account of the loss of privacy and right to their data. Furthermore, the terms and conditions governing major platforms are not subject to meaningful refusal or negotiation.

In this sense, the model of digital participation itself embodies domination. Access to essential online platforms and services is conditional upon the renouncement of personal data, leaving

individuals unable to exercise genuine control over their informational privacy. In contemporary life, abstaining from digital communication, email, or smartphone use is hardly feasible. Even those who might wish to abstain in private life are often required to participate by employers or institutions. Thus, the very conditions of participation in the digital public sphere compel individuals to live under the *arbitrary* power of those who control their data.

The power to interfere is arbitrary if it fulfils at least one of the conditions for arbitrariness as defined above in the chapter 'Freedom as non-domination' (chapter 2). In this case all three of these conditions have been satisfied: The interests of the individuals being affected by the *quid pro quo* of digital services are not being served by the parties setting up the agreements as the individual. Neither can individuals meaningfully contest the terms and conditions of platforms or services they wish to use, nor can any given individual meaningfully hold surveillance capitalist firms accountable for their loss of privacy. As such, the firms effectively dominate the individual users, leading to a situation in which the individual users can be said to be unfree.

Having shown that the process by which users lose the rights to their data is a form of domination, I will continue in the section below to consider what a loss of privacy entails for any given individual. I aim to show with the help of an example that the absence of privacy can expose an individual to forms of domination they would otherwise not be exposed to. As such I will argue that privacy can be an effective shield for any given individual against attempts at manipulation by others.

4.3 Loss of privacy, data inference and domination on a smaller scale

In general, access to data points about any individual can give other actors the ability to share the knowledge contained within these data points, either willingly or unwillingly. These data points in question could very well be harmless, but the more data some other actor has about an individual the more likely that the leaking of such data might be a detriment to the individual's ability to continue unhindered with their daily life. Worth highlighting in the case of digital privacy is the fact that although many data points about any given individual might be meaningless, it is often possible to infer more information from any given number of data points than is contained within the data points themselves.

For the sake of argument, let us assume that we have two individuals: A and B. A knows about B that B visits some specific location P every week. For most possible locations P, this could by itself be a harmless fact about B. However, this specific location P is a medical clinic specialized in addiction treatment. In our current example let us suppose that A knows that P is an addiction clinic. With just these two data points, A can infer that B is likely undergoing treatment for an addiction.

In the example above, the inference from just the two data points – that person B is likely struggling with addiction – gives some leverage or power over B to whichever other actor holds this information. Although to most people person B is of no interest, this information could be valuable to, for example, their employer, insurer, or an advertising platform. Any person A who made this inference about person B could share the inferred information with entities interested in person B. If A knows about B's visits to clinic P, and A is in a position where they can share

this information with others, furthermore supposing that such interested entities exist, A is in a position where they can *arbitrarily* interfere in the life of B. A's capability to interfere in the life of B is arbitrary as B has no way to contest A sharing this knowledge and can neither hold A accountable for their actions. As the knowledge about B's visits to clinic P is something that A inferred themselves, A could be considered to own this knowledge as can share this knowledge with others if they so desire. Supposing for the sake of argument that there are parties interested in B's struggles with addiction, and that these parties would treat B differently if they learned of their problems, A can be said to be able to interfere in the life of B. For example, we might imagine that an insurer would ask for more contribution or outright refuse B as a client, or B's employer that would think twice before giving more responsibilities to B or outright fire them. All of this combined, we can conclude that in republican terms individual B is dominated by A, as A has some form of power to arbitrarily influence B's reputation, opportunities or autonomy.

Even if holders of such data like A never act upon their power over person B, the mere fact that they could exploit this knowledge places B in a position where they are being dominated. Whether the individual is aware that their private struggle is known to external actors or not, these actors could interfere with the life of the individual arbitrarily as they do not merely know about the individual's struggle with addiction, they own this knowledge. The danger here is not so much the loss of secrecy, but the creation of a structural relation of vulnerability. The individual must depend upon the goodwill or restraint of whomsoever controls the data about them, which is precisely the sort of condition that Pettit (2016) identifies as domination – and thus the negation of freedom.

4.4 Loss of privacy, data inference and domination on a larger scale

On a larger scale, individuals leave data points any time they access the internet or engage with products and services of surveillance capitalist firms. Although many points of data generated in this way are arguably meaningless and harmless on their own, the combination of thousands of small 'crumbs' of data can reveal significantly more than is contained within the data points about any given individual's life, thoughts and feelings.

Arguably an individual might want to keep all this information to him or herself, or – at least – the individual wishes to decide with whom he or she is willing to share personal information. I hope to have shown with the example above that even a very small amount of data points could already reveal things about an individual's life that they would rather keep to themselves. In practice, however, almost any digital interaction is monitored and the data about your usage of such products is being recorded, processed and stored in a personalized profile. Furthermore, even if you are not using but merely carrying electronic devices, your location data is very likely still being tracked, be it with GPS, cellular data or even which Wi-Fi networks your device is registering nearby. The default settings of most electronic devices allow outsiders to uninterruptedly track your location, send this information to servers of private entities and to store this information indefinitely if these private entities wish. Even if such an entity has no intention at all to do any harm, the accessibility of this data by this entity might reveal private information that one doesn't want to share with an unknown and/or commercial outsider.

Whether an individual does or doesn't realize their whereabouts are tracked, it should be realized that external commercial parties know a lot about themself and those around them.

From a republican perspective this harvesting of data points about any given individual's life is problematic because it gives those who hold such data the ability to interfere with the individual's life at an arbitrary basis. The individual has no say into what the owner does with the data about them. The owners could sell the data, it might get leaked in a security breach or the data owners might share personal information with governmental agencies. Even in the case that the owners of the data in question keep it completely to themselves, this creates a power imbalance between the holder and subject of the data. By making use of 'free' internet services, the individual generates new data points about themselves without any rights of ownership and thus has no say as to what will happen with that data after it has been collected.

4.5 Privacy as a shield against further domination

Apart from domination as a direct result of the loss of privacy, individuals might also be exposed to further domination because of their lack of privacy. In cases where a lot of information about any given individual is in the hands of external actors, this leaves the individual vulnerable to further forms of domination. The data points about any such individual could be used to either manipulate or exploit the individual; the topics of the following two chapters.

The opposite however – enjoying privacy – shields the individual against such further forms of domination (Roberts 2022, pp. 39-41). This is best explained by showing what a lack of privacy might entail for those in possession of personal information:

> *"loss of privacy might enable others to manipulate our decision-making in other aspects of our lives – the acquisition of information about a person's fears or aspirations, as a consequence of idle gossip with a mutual acquaintance, for example – and to do so in ways that might have a significant effect on our autonomy. Such information could also be shared with others who might attempt to manipulate you so that you make decisions that serve their ends"* (Robert 2022, p. 50).

If individual A wants to do *P* and not *Q* for reason M, knowledge of reason M might enable corporate actor B to shift A's plan of action towards *Q*. For B to able to change the course of action that A will pursue, knowledge about A's reason M is valuable to B. If B attains knowledge of M this would at the least be somewhat useful to B's goal to make A do *Q* instead of *P*, since A wants *P* because of M. If B can act upon, change, or replace reason M with some other reason, they might very well be able to shift A's course of action. Privacy in this example would be A's control or ability over whether corporate actor B can access their reason M to do *P*. If A can hide M from B, they are in a sense freer to pursue *P* without interference from B. For in the case that no other actor has access to relevant information about individual A such as M, A is guaranteed that they are not exposed to arbitrary interference which uses their data against them.

This argument applies to any case of domination in which individual A is being dominated by corporate actor B, where B is enabled in their interference with A on account of their knowledge

M about A. In all such cases privacy – the shielding of knowledge M outside of the view of B – would prevent A from being dominated. Since surveillance capitalism is driven by the collection and processing of data about individuals, privacy should be considered the ideal way to prevent domination of individuals by corporate actors.

4.6 Answering the sub-question

To wrap up this section on privacy I can answer the sub-question affirmatively. Individual privacy loss occurs at a level that is hitherto unseen in human history and does amount to domination. Furthermore, this loss of privacy exposes individuals to the possibility of further domination, such as exemplified especially in the chapter on manipulation. In the next chapter I will first look though at exploitation, which is mainly enabled by the power differences between individuals and corporate actors.

5 Exploitation

In this chapter, I will evaluate the possible harms done on an individual level that could be classified as exploitation from a republican perspective to answer the following question:

Does exploitation of individuals occur when they engage with the platforms of surveillance capitalist firms in a way that amounts to domination?

After giving a working definition of exploitation to which I am indebted to Benn and Lazar (2021), I will go over 3 different areas in which surveillance capitalism may be considered to dominate individual users. In turn these are power differences between individual users and corporate actors, the absence of alternatives for individuals to surveillance capitalist platforms, and the possible objectification and commodification of the users themselves. I will investigate whether surveillance capitalism can be said to exploit the individual users of their platforms and services and a way that would be considered to amount to domination.

5.1 Defining Exploitation

Benn and Lazar define exploitation as occurring

> *"when one party to an ostensibly voluntary agreement intentionally takes advantage of a relevant and significant asymmetry of knowledge, power, or resources to offer the other party terms of exchange to which they agree but would never accept were they more symmetrically situated in that respect"* (2021, p. 135).

I have condensed this definition for the purposes of the current thesis to the following:

Formal definition:

- A wants to do *P*
- B makes A to do *Q* whilst A wants *P*

Roughly speaking, exploitation in the context of surveillance capitalism occurs when a surveillance corporation changes the individual's behavior *without* changing the individual's desires. A corporation uses their much larger knowledge, power, or resources to compel the individual to agree to a certain arrangement or change their behavior *against their own desire.* It differs in the latter sense from manipulation, which I define to occur when an individual changes their behavior because their desires, beliefs or goals have been altered on account of interference by a surveillance corporation.

For exploitation in this sense to be considered domination, this interference on account of the corporate actor(s) must be considered arbitrary as described in the chapter above on Freedom as non-domination. For forms of exploitation to amount to domination it should be considered an interference in the life of individuals, which does not serve the interest of the affected individuals, which the individuals can neither contest and nor can they hold the corporate actors accountable. It would seem obvious that exploitation as defined above would amount to interference, however, whether exploitation in this sense *de facto* obtains and could be considered arbitrary is the subject of the remainder of this chapter.

5.2 Power differences

Benn and Lazar (2021) argue that on an individual level not many would have a 'strong complaint' that they are being exploited in their use of online services. Individual users gain access to some services, which are free regarding monetary cost, and pay by data. Whether any given individual is aware of this cost or not, this could be seen as a voluntary exchange (Benn and Lazar 2021, pp. 135–36). In any case, if I were to argue from a point that such an exchange would be involuntary or forced, there would be strong burden on me to provide backing for such a claim, preferably backed by empirical data. As this falls without the scope of the current thesis, I would instead like to question whether an individual's subjective sense of exploitation is necessary for determining whether exploitation – in a way that amounts to domination – in fact occurs. One could ask whether individuals would still consent to these ostensibly voluntary agreements if they were fully aware of the asymmetries of knowledge, power, and resources at play, or, more precisely, whether the users would object to there being no way for them to use online services without renouncing their behavioral data. I will take it to be self-evident that in the context of surveillance capitalism; the asymmetries of power are so vast that individuals have virtually no bargaining power compared to any given corporate actor.

I wish to highlight this imbalance of power because although itself not necessarily problematic to republicans, it means that any interference in the life of individuals on the part of corporations is – in the absence of strong government regulation – uncontestable by individuals, and neither can individuals realistically hold corporate actors accountable for their actions. In almost all cases where an individual would come into conflict with a surveillance capitalist corporation, the individual stands at a strong disadvantage.

5.3 Absence of alternatives

The imbalance of power between the individual and a corporation is further entrenched by the absence of meaningful alternatives. By this I mean that digital platforms have in many cases become indispensable for work, communication, and social participation, leaving individuals with little practical option but to accept the terms of service of the platforms of surveillance capitalism. This dependence is further amplified by social pressures if one's peers communicate primarily via WhatsApp or Instagram, opting out carries significant social costs. Empirical studies reinforce this point, with Zuboff citing research in which students reported that it was "*impossible to imagine even casual social participation without social media*" (Moeller n.d. via Zuboff 2019, p. 280). These dependencies are no accident, and monopolistic behavior, in which for certain areas of life a certain service becomes indispensable, is desirable to corporations and something that they actively strive to achieve (Zuboff 2019, pp. 281-84).

The asymmetry of power becomes especially stark when corporations exercise unilateral control over the service agreements users might agree to before they can make use of the service in question. Furthermore, many of such companies reserve the right to terminate accounts which are seen to break the terms of service without any real way for the affected users to contest their exclusion, effectively ostracizing individuals from vital digital infrastructures. One widely reported case involved users that lost access to years of data, emails, and photographs when Google suspended his account without recourse. In one case, a person,

‘Cleroth’ (not his real name), was denied access to his Google account as Google had determined he had broken their terms of service, though they didn't explain exactly what had happened. It was also made clear that his account wouldn't be reinstated (Stokel-Walker 2020). It is certainly conceivable that ‘Cleroth’ indeed had seriously infringed Google terms of service, but it is impossible to defend oneself if there is no clear accusation.

Even when such power is not exercised, the mere possibility of arbitrary exclusion constitutes a form of domination, undermining individual autonomy. When it is exercised, individuals are left powerless against the might of corporate decision-making (Oldenbourg 2022, 389).

5.4 Objectification and commodification of users

At its core, surveillance capitalism is structured around the extraction, processing, and commodification of human experience. Every click, search, and interaction is appropriated as raw material, not for the benefit of the individual but to maximize corporate profit. Users are reduced to data sources – objects to be analyzed, predicted, and nudged – rather than agents able to shape their own choices (Zuboff, 2019, 237–39). This practice undermines republican freedom, which requires protection from the arbitrary power of others. Surveillance capitalism places individuals in a position of dependency, where corporations can unilaterally determine how their data is collected, interpreted, and exploited. Such arrangements are not relations between equals but relations of domination: individuals are manipulated as resources rather than engaged as participants in fair and contestable terms. Even when users gain access to valuable services, their freedom is compromised, since they remain vulnerable to the unchecked discretion of powerful corporate actors.

Finally, the structural asymmetry of surveillance capitalism leaves individuals unable to exercise genuine autonomous choice. Privacy settings are cumbersome and only partially effective. Moreover, one’s privacy depends not only on personal actions but also on the behavior of others; data shared by friends and acquaintances often suffices to reconstruct intimate profiles (Véliz, 88–96). In this way, surveillance capitalism ensures that even the most privacy-conscious individuals cannot truly opt out, further entrenching dependence and undermining both autonomy and dignity.

5.5 Answering the sub-question

To wrap up this section on exploitation I can answer the sub-question affirmatively. Exploitation of individuals does happen insofar as the individuals in question engage with the platforms or services of surveillance capitalist firms, and especially if they have become reliant upon them.

6 Manipulation

This chapter will attempt to answer the following question:

Does manipulation of individuals occur when they engage with the platforms of surveillance capitalist firms in a way that amounts to domination?

I will investigate whether individuals are dominated by corporations under surveillance capitalism by being manipulated. To start I will provide a working definition of manipulation, followed by a subdivision of manipulation in two different types. The remainder of this chapter will focus on investigating whether individuals are being manipulated by surveillance capitalist firms in a way that amounts to domination.

6.1 Defining manipulation

Benn and Lazar start by giving a sufficient condition for manipulation.

> *"Manipulation involves (though may not be exhausted by) undermining an individual's decision-making power—for example, preying on their emotions, their momentary whims, or their reliance on cognitive biases and heuristics—in order to change their behaviour"* (2021, p. 139).

Formal definition:

- A wants to do *P*
- B knows A wants to do *P*
- B makes A want to do *Q*
- A does *Q*

Roughly speaking, I consider manipulation to occur when individual A initially wants to do *P*, but due to interference from corporate actor B changes their desire to *Q*. B having knowledge about A's desire for *P* and having the potency to change A's desire to any *Q* are required for B to be able to change A's desire.

For manipulation to be considered domination in a republican framework, corporate actor B must have the capacity to arbitrarily change the desires of individual A. As laid out in the chapter on freedom as non-domination above, arbitrariness here consists in the exercise of power that fails to serve the interests of those subjected to it, that is not contestable by them, and that is not constrained by publicly shared standards of justification.

For the purposes of this chapter, I consider manipulation to occur under surveillance capitalism in two distinct ways. Firstly, direct manipulation occurs when attempts are made through the platforms or services of surveillance capitalists to influence individuals, a prime example of which would be advertising. Secondly, surveillance capitalist systems might indirectly influence the behavior of individuals through the personalization of content shown to the individual.

I will argue that the practices of surveillance capitalism *de facto* expose individuals to manipulation by surveillance firms and will evaluate whether this manipulation could be considered to amount to domination. To do so, I will categorize manipulation to be either direct or indirect.

6.2 Attempts at direct manipulation

Firstly, there is direct manipulation, which occurs when a corporation actively interferes with the choices that an individual makes, or at least attempts to do so, through changing the individual's desires.

There are multiple ways in which surveillance capitalist systems might attempt to manipulate users, but I want to focus here mainly on the most common and pervasive of all of those: advertising. As a small recap from the introduction above, advertisements are the main source of income of surveillance capitalism as a system. Through the gathering and processing of data about individuals it is possible to tailor advertisements to the audience that will see them with great precision. Since big tech firms know so much about their users, they are in prime position to use this information to sell targeted messages to the audiences that are most susceptible to them in ways that are most likely to be effective.

I consider advertising to fall under the denominator of manipulation since it actively attempts to steer any given individual's desire to a certain product, service or other goal. If I am being served an advertisement by a corporation to buy a specific watch, the advertisement is actively trying to steer my behavior to make me buy this specific watch.

In a republican framework, personalized advertising as such does not need to amount to domination. Advertisements have been around for a long time and the tailored messages served to individuals through online media might be considered an evolution of an already-existing system. Benn and Lazar highlight that the most problematic result of surveillance capitalist advertising is the influence one can wield on larger scales by buying the services of the surveillance capitalist firms. As such, Benn and Lazar note that direct manipulation can be shown to have tangible effects on a larger scale. To quote: "*the tools of Automated Influence seem to allow those who can wield them an outsized ability to influence populations to advance their goals"* (Benn and Lazar 2021, p.142). However, they argue that it will be much harder to show nefarious effects from attempts at manipulation on an individual level. This is because advertisements and nudging have a chance to work on any given individual. Even if this chance is just a few percentage points, on large scales this can entail that large groups of people are effectively manipulated (Benn and Lazar 2021, pp. 140-41). As I am arguing here from an individual level, such dangers fall outside of the scope of the current thesis. Individuals can hardly be said to be manipulated and thus dominated by an attempt at nudging that has a small chance of succeeding, so I will not pursue such arguments any further here.

6.3 Attempts at indirect manipulation

Secondly, I will consider indirect manipulation, which occurs when the choices an individual makes are being *indirectly* shaped by interference on behalf of a corporate actor. An example of indirect manipulation would be when one's actions change due to changes in one's

worldview due to algorithmically served content. This could happen when one sees lots of stories about refugees drowning in the Mediterranean Sea, making one want to vote for politicians with a welcoming stance towards refugees. If on the other hand one were to be served content about crimes being committed by refugees near one's location, one might instead want to vote for politicians aiming to block refugees from entering my country. In this way, although the algorithms curating the news feed would be purely aimed at making everyone engage more with the news feed, whatever any given individual is shown might very well indirectly manipulate them in different ways.

The focus of the remainder of this chapter is that many sources of information that individuals consume are 'personalized', tailored to one's individual tastes and interests based on what the personalizing algorithms know about any given individual. This may not be directly manipulative, but what information is accessible to any given individual will influence how they view the world. This part of the indirect manipulation focusses on precisely this aspect, where the content that any given individual engages with on platforms from surveillance capitalists is selected by an algorithm. To name some examples: it differs starkly per person what videos YouTube recommends to them, similarly, search results that Google gives for the exact same search prompt as another user can give starkly different results, the *timelines* or *feeds* of users on Instagram and Facebook are also not only personal but tailored to the specific individual by an algorithm.

Many sources of information, entertainment, news, or other content are tailoring algorithmically what the user sees. The fact that what we are all interested in differs from person to person, and as such, what makes one click, look and stay engaged with whatever platform also differs. This latter motivation is the main source of what any given user sees on their feed. Companies are after all aiming to make a profit, and your attention is worth money. The longer any given platform can keep your attention inside the platform, the better. Due to this incentive, users are being served content by algorithms that are trained to keep the individual engaged.

Whenever any individual browses through algorithmically generated feeds, an outside actor controls or at least steers what information is available to the individual, in an arguably arbitrary way as the goal here is to keep the user engaged, which is a goal of the platform in question, not of the individual.

This outside actor could be said to dominate individuals engaged with such a platform, by controlling the informational environment through which the individual exercises judgment. The collection and algorithmic processing of personal data endow corporate actors with the capacity to tailor individuals precisely to their cravings and impulses. Control of big platforms not only gives a lot of data about individuals to corporations, but such control also endows the corporations to shape what information users engage with on their platforms. Although no given platform is truly inescapable, for many different types of activities certain platforms come close. For example, if one is in search of a new job LinkedIn seems the obvious place to start, or if one searches for a short video with an explanation for something, YouTube is the default starting place. Many people *de facto* use and rely upon platforms that serve algorithmically curated content. I would argue that any such individual that relies upon a

platform like that could be said to experience interference in the way they gather information. A platform such as LinkedIn or YouTube is almost part of the environment in which people go about their daily business. Only in these cases are there outside companies in full control, actively manipulating this environment to benefit themselves rather than the individuals operating within these digital environments.

This power to intervene is arbitrary in all three ways that I defined in the chapter above on freedom as non-domination. Firstly, the interests of the affected party – being the individual users – are not being served by the interference on behalf of the surveillance capitalist firms when they interfere with information that this person can take in. The interest of companies lies in making more profit. Secondly, there is no real way that the users can contest this interference. They might just 'opt out', as in not use the services of the surveillance capitalist firms or abstain from use of platforms which are algorithmically filled with content. However, it is hard to truly abstain, and on the platforms of surveillance firms there is no way that an individual can fully avoid the algorithmic personalization of content. Thirdly, there is hardly any accountability. Algorithmic personalization is not something that any individual user can hold a large company accountable for. Alone this would be a story of David against Goliath, where the tech companies have dedicated legal teams to ensure that they are defended in court when any threat to their operations appears from the legal system. Furthermore, the individual cannot even know how the algorithmic personalization of content specifically works. The underlying algorithms are essential business secrets, and often not even governments of individuals consuming personalized content can access the inner workings of the algorithms at play.

As such I feel confident to conclude that provided that any given individual is in some form reliant upon engaging with the platforms or services of surveillance capitalist firms, this individual being exposed to subtle forms of indirect manipulation is a given. Whether truly manipulated or not, the wrong here lies less in the contingent outcomes of manipulation and more in the standing vulnerability of individuals to such arbitrary control. Even if the filtering of information were to coincide with a user's preferences or even to benefit them in certain cases, the structural relation would remain one of domination. For as long as their sources of information are algorithmically curated without mechanisms that reliably ensure alignment with the individual's interests, and the individual can neither contest the curation or hold whichever party responsible accountable, individuals are exposed to arbitrary interference and hence dominated by whichever corporate actor in question controls the informational environment the individual engages with.

Thus, surveillance capitalism undermines individual liberty as non-domination in the sense of manipulation. By monopolizing the channels through which individuals acquire beliefs and form judgments, it renders them perpetually dependent on powers that operate beyond their reach. The epistemic environment ceases to be a common space structured by contestable norms and instead becomes an instrument wielded arbitrarily by corporate entities. In a republican framework this clearly amounts to domination.

6.4 Answering the sub-question

To wrap up this section on manipulation I can answer the sub-question affirmatively. Although direct manipulation can hardly be said to occur in a relevant sense to speak of domination, indirect manipulation happens insofar as the individuals in question engage with and especially if they have become reliant upon the platforms or services of surveillance capitalist firms.

7 Conclusion

This thesis set out to answer the following central question:

> *To what extent can the corporate practices of surveillance capitalism be shown to interfere with individual freedom when analyzed through the republican concept of non-domination?*

By examining surveillance capitalism through the lens of Philip Pettit's neo-republican theory (2016), and by focusing explicitly on harms at the level of individual users, the analysis has sought to determine whether the power exercised by surveillance-capitalist firms amounts to domination rather than merely to benign or permissible influence.

The core claim defended throughout this thesis is that surveillance capitalism systematically places individuals in relationships of arbitrary power. Even when corporate actors do not actively interfere with users' choices, they possess an extensive and largely incontestable capacity to interfere with any individual that is reliant upon the services or platforms provided by said corporate actors. This omnipresent capacity for interference – enabled by data collection, processing and algorithmic curation of content served to individuals – suffices, on a republican account, to undermine individual freedom. Freedom as non-domination is not secured by the absence of interference alone, but by the absence of dependence on the goodwill or restraint of others. Surveillance capitalism fails to meet this standard.

The analysis proceeded by examining three domains of potential wrongdoing: privacy, exploitation, and manipulation. First, it was argued that the loss of privacy experienced by individuals under surveillance capitalism facilitates domination. Individuals are effectively compelled to renounce control over personal data to participate in essential digital infrastructures, without meaningful opportunities to contest the terms of data collection or to hold corporate actors accountable for subsequent uses of that data. The resulting asymmetry of informational power renders individuals structurally vulnerable, even if no concrete harm would materialize. The erosion of privacy itself amounts to domination but furthermore exposes affected individuals to domination in other areas.

Second, the thesis argued that the economic relations between users and surveillance-capitalist firms plausibly amount to exploitation in a way that constitutes domination. Although individual users may not experience the exchange of data for services as coercive or unfair, this subjective assessment is insufficient from a republican perspective. The absence of realistic alternatives, combined with vast disparities in power, knowledge, and resources, means that individuals are unable to refuse, renegotiate, or contest the terms of participation. Moreover,

the commodification of human experience positions users not as equal participants in a mutually beneficial exchange, but as the source of raw data for profit-driven systems over which they exercise no meaningful control.

Third, the analysis of manipulation distinguishes between direct and indirect forms. While direct attempts at manipulation, such as targeted advertising, cannot be shown to reasonably involve domination, indirect manipulation through algorithmic curation of informational environments does. By shaping what information individuals encounter, and by doing so according to hidden and profit-driven criteria, surveillance-capitalist platforms exercise control over the conditions under which individuals form beliefs, preferences, and judgments. Because this control is neither transparent, contestable, nor accountable, it constitutes a form of arbitrary interference incompatible with republican freedom.

Taken together, these findings support an affirmative answer to the central research question. Surveillance capitalism undermines individual freedom as non-domination not primarily through isolated acts of coercion or deception, but through the creation of structural relations in which individuals are subject to unchecked corporate power. Even when users benefit from digital services, or when corporate interference aligns with users' immediate preferences, the underlying condition of dependence remains. In republican terms, this condition is sufficient to establish domination.

At the same time, this thesis has important limitations. Its focus has been deliberately confined to individual-level harms, abstracting from broader societal consequences such as democratic erosion, political polarization, or collective epistemic degradation, which were the focus of the article by Benn and Lazar (2021). Moreover, this thesis stops at concluding that surveillance capitalism as a system harms individual freedom. What – if anything – should be done about this conclusion is something that is deliberately left outside of the scope of the current work. These limitations are not defects but reflect a methodological choice: to clarify whether surveillance capitalism is objectionable on an individual level in principle from a republican perspective, before turning to questions of remedy.

The broader implication of this analysis is that existing liberal frameworks, which emphasize consent, utility, or non-interference, may be insufficient to capture what is morally troubling about surveillance capitalism. A republican perspective reveals that the central wrong lies in the concentration of arbitrary power over individuals' lives, choices, and informational environments in the hands of corporate actors. How individuals or society at large should respond to such a finding is a question left open. Since individuals have little choice but to be subjected to the arbitrary power of surveillance capitalism, future research might explore concrete institutional responses – such as data governance regimes, platform accountability mechanisms, or the redesign of digital infrastructures – to better secure freedom as non-domination in the digital age.

References

Benn, Claire, and Seth Lazar. "What's Wrong with Automated Influence." *Canadian Journal of Philosophy*, 2021. https://doi.org/10.1017/can.2021.23.

Business of Apps. 2025. "Signal Statistics." Accessed December 16, 2025. https://www.businessofapps.com/data/signal-statistics/.

Cadwalladr, Carole, and Emma Graham-Harrison. "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." *The Guardian*, March 17, 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Fuchs, Christian, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval. *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*. Vol. 16. New York: Routledge, 2012.

Google**.** 2025. *"Privacy Policy."* Accessed December 17, 2025. https://policies.google.com/privacy

Lazar, Seth. "Power and AI: Nature and Justification." In *The Oxford Handbook of AI Governance*, edited by Justin B. Bullock et al. Oxford: Oxford University Press, forthcoming.

McCammon, Richard C. "Domination." In *The Stanford Encyclopedia of Philosophy*, Winter 2018 Edition, edited by Edward N. Zalta. https://plato.stanford.edu/archives/win2018/entries/domination/.

Mill, John Stuart. "Introductory." In *On Liberty*, 7–30. Cambridge Library Collection - Philosophy. Cambridge: Cambridge University Press, 2011.

Moeller, Susan D. n.d. *"The World Unplugged."* Accessed December 17, 2025. https://theworldunplugged.wordpress.com/.

Oldenbourg, Andreas. "Digital Freedom and Corporate Power in Social Media." *Critical Review of International Social and Political Philosophy* 27, no. 3 (2024): 383–404. https://doi.org/10.1080/13698230.2022.2113229

Pettit, Philip. *On the People's Terms: A Republican Theory and Model of Democracy*. Cambridge: Cambridge University Press, 2012.

Pettit, Philip**.** "A Brief History of Liberty—And Its Lessons." *Journal of Human Development and Capabilities* 17, no. 1 (2016): 5–21. https://doi.org/10.1080/19452829.2015.1127502

Roberts, Andrew. *Privacy in the Republic*. 1st ed. New Delhi: Routledge India, 2022. https://doi.org/10.4324/9781003079804.

Stahl, Bernd Carsten, Doris Schroeder, and Raúl Rodríguez. “Surveillance Capitalism.” In *Ethics of Artificial Intelligence*, 2023. SpringerBriefs in Research and Innovation Governance.

StatCounter GlobalStats. 2025. “Browser Market Share Worldwide.” Accessed December 16, 2025. https://gs.statcounter.com/browser-market-share.

Stokel-Walker, Chris. “Google Users Locked Out After Years.” *Business Insider*, October 2020. https://www.businessinsider.com/google-users-locked-out-after-years-2020-10.

Véliz, Carissa. *Privacy Is Power: Why and How You Should Take Back Control of Your Data*. Brooklyn, NY: Melville House Publishing, 2021.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.