2021

ERROR 404 CONSENT NOT FOUND: The Problem with Exchanging Privacy for Accessing Modern Technological Goods & Services

Seth Wade

ERROR 404 CONSENT NOT FOUND

The Problem with Exchanging Privacy for Accessing Modern Technological Goods & Services

Seth Wade
Honors Thesis: Philosophy
Advisor: Randall Harp
5/19/2021

Table of Contents:

Introduction

Man always kills the thing he loves. And so we the pioneers have killed our wilderness. Some say we had to. Be that as it may, I am glad I shall never be young without wild country to be young in.

— Aldo Leopold, *A Sand County Almanac*

A 2018 report in *Nature* estimated that less than a quarter of Earth's wilderness remains. Wilderness, understood in the report as areas free of industrial scale activities and other human pressures which result in significant biophysical disturbance, are important and necessary to protect for many reasons. Aside from their vital role in biodiversity conservation and scientific research, there is innate value in protecting such spaces where nature flourishes on its own—to let forests grow un-sculpted, to let plants and animals thrive without modification or annihilation.[1] These ecosystems foster life unique and only born in these spaces: there is no such thing as an artificial wild. In this understanding, the wilds are not raw materials to seize, exploit, or consume—wilds are spaces where natural flora and fauna must be allowed to develop without undue influence from human beings.

No report has attempted to estimate the loss of our mental wilds. By mental wilds, I am referring to our private mental space which protects our natural human autonomy—otherwise referred to as privacy. One of the reasons why privacy as protection from undue external influences

[1] It is estimated that around 77% of land (excluding Antarctica) and 87% of the ocean has been modified by the direct effects of human activities (Watson et al 2018, para. 1). During a 2017 conference in Vatican City, where scientists announced that an estimated that 50% of all species on Earth could go extinct by the end of the century, biologist Peter Raven remarked: "The extinctions we face pose an even greater threat to civilization than climate change, for the simple reason they are irreversible" (Haro 2017, para. 2).

is undertheorized is because privacy has traditionally been conceived as not letting certain information out: not letting others access our personal information. In the age of surveillance capitalism, however, privacy is also about not letting certain information be allowed to come back in: not letting our personal information be used to exert undue influence over us. When we engage with modern technological goods and services (which we require to fulfill our modern personhood) our human experience is claimed by corporations as free raw material for their hidden commercial practices of extraction, prediction, and sales. This information is necessary for the tools of instrumentarianism which saturate the digital economy. Instrumentarianism is the power to know and shape human behavior toward other's ends. By modifying our thoughts and behaviors (often without our awareness), instrumentarian tools complicate our ability to think and act autonomously. And in order to be autonomous, we need space independent from undue influence from others. Privacy, like Earth's wilderness, provides crucial distance. Like the precious flora and fauna found in Earth's wilderness, there is value in human autonomy in its own right. We don't want all of Earth to be a beautifully arranged garden just like we don't want ourselves living as efficiently orchestrated automatons; as we value nature growing according to its own designs, so do we value autonomy.

Surveillance capitalism yields many harms, but its creation of instrumentarianism is arguably the most worrying. Currently these tools complicate our autonomy in inappropriate ways, but the potential threat they pose to our autonomy makes them intolerable. Considering privacy's essential role in developing our autonomy, as well as the existence of a thriving market centered around disrupting our autonomy through our diminished privacy, it is important that whatever sort of logic we are using to support an exchange that removes our privacy prove justified.

While philosophers continue to debate how best to reconcile emerging technologies with our desire for privacy, no one is really addressing the solution society has already tacitly accepted: that it is okay to infringe upon an individual's privacy in exchange for accessing modern technological goods and services, so long as the individual consents. Social contract theory holds that individuals consent either explicitly or implicitly by surrendering some of their freedoms to an authority in exchange for their other rights or to maintain social order. In attempting to identify the social contract negotiating our privacy and access to modern technological goods and services, I adopt the term "technosocial" from Shannon Vallor, who I will later explain makes the convincing case that a modern virtue ethics should explicitly address our relationship with modern technology.

Perhaps the most pervasive and well-known form of this technosocial contract is the ritual of clicking "I Agree" to whatever terms and conditions any given technological service or device is imposing upon you. Legal experts label these terms-of-service agreements as "contracts of adhesion" because they impose take-it-or-leave-it conditions on users whether they like it or not, often referring to them as "click-wrap" because most people get wrapped in these oppressive contract terms without ever reading the agreement (Zuboff 2019, 48). And despite studies[2] determining that the vast majority of users don't read before clicking, most courts have upheld the legitimacy of click-wrap agreements. Even the General Data Protection Regulation (GDPR) passed by the European Union in 2016—currently the strongest and boldest privacy legislation protecting the data of individuals using the technological devices and services we've become so reliant on—still hinges on this basic technosocial contract. So long as you consent, then

[2] One study conducted by Carnegie Mellon in 2008 calculated that a reasonable reading of all the privacy policies that one encounters in a year would require seventy-six full workdays at a national opportunity cost of $781 billion (Zuboff 2019, 50).

exchanging your privacy to access the basic goods and services you need to compete and thrive in modern life is justified.

I argue this exchange remains unjustified because meaningful consent cannot be formed through our current technosocial contract. Concisely put, my argument runs as follows:

A. Our current technosocial contract justifies the exchange of an individual's privacy for access to modern technological goods and services by requiring an individual's consent.

B. As modern human beings, we require access to modern technological goods and services to enjoy our modern personhood, to enjoy the goods of modern life and fulfill our autonomy. No one can be reasonably expected to decline the goods of modern life; to click disagree on our modern personhood is to endure an unbearable harm.

C. Modern technological goods and services operate under an exploitative, harmful economic order best understood as surveillance capitalism. This system profoundly diminishes our privacy. This loss of privacy allows others access to our autonomy through instrumentarianism. Instrumentarian tools modify our thoughts and behaviors, often without our awareness; it is through these tools that our mental wilds are cut away and our autonomy becomes vulnerable. To have one's autonomy disrupted and made vulnerable such a way is to endure an intolerable harm.

D. Given B and C, it is problematic to exchange privacy for access to modern technological goods and services. If an individual declines to consent, they are denied the means to realize modern personhood and fulfill their autonomy—an unbearable harm. But if an individual accepts, then they're entering an exploitative system of various harms where instrumentarian tools endanger their autonomy. Choosing

between these options doesn't seem like much of a choice; this exchange doesn't feel morally transformative.

E. Leading theories on consent agree with D, though none agree on what makes this exchange problematic. Although this exchange doesn't fit the narrow definition of coercion in these theories, this is the most appropriate term. Denying an individual's access to modern personhood pushes this exchange toward being a coercive offer, while there is also something inherently coercive about requiring individuals autonomously consent to endanger their autonomy on a marketplace built around disrupting autonomy.

F. Consent and coercion are incompatible. I argue we have good reason to regard this exchange as coercive, meaning it is incapable of producing consent. Furthermore, even if we do not want to use the term coercion to describe this exchange, leading theories on consent still view this exchange as failing to be morally transformative—meaning this exchange is still incapable of producing meaningful consent.

G. Because of E and F, our technosocial contract as stated in A remains unjustified: when exchanging our privacy for access to modern technological goods and services, it cannot be said that we truly consent.

Part I: Privacy & Autonomy

PRIVACY AS PROTECTION FROM UNDUE EXTERNAL INFLUENCES

Though scholars continue to revise our understanding of privacy, humans have always required privacy to feel human. The need for privacy has been appreciated in different ways from culture to culture. During the Heian period in ancient Japan, ladies in waiting used special half-sewn curtains at the entrance of their bedchamber: objects could pass through the bottom, while the prying eyes of their suitors could be kept in check.[3] Ancient Greek philosophers debated the distinction between 'outer' and 'inner', public and private, and society and solitude (Holvast 2009, 15). In Catholicism, priests listen to confessions in private booths called confessionals, bound by God to never disclose anything they've heard. While differences in how privacy is appreciated continue to this day, general trends can still be gleaned from the long history of humanity's appreciation for privacy. In his essay chronicling this history, Jan Holvast identifies three such trends: 1) that the needs for one's privacy has traditionally been balanced against the needs of society, 2) that technology has typically been understood as presenting challenges for privacy, and 3) that privacy has always been seen as something under attack. Yet privacy has also been historically difficult to define. In the last few centuries, this has been largely due to advancements in technology outpacing our philosophical and legal scholarship around our concept of privacy, resulting in obvious and devastating invasions of privacy being not only legal but difficult to defend against.

[3]Sei Shōnagon, writer and court lady of Empress Consort Teishi, called it the 'curtain of the State', and it did not guarantee complete privacy—as Robin Duke notes during his introduction to a translation of her work: "Sei Shōnagon and her fellow ladies in waiting were forever ensconced behind their screens, overhearing and overheard" (Duke 1979, 20).

Despite being outpaced, researchers across disciplines have given us many useful definitions of privacy. Philosopher Charles Fried conceived of privacy as an intrinsic value, arguing that privacy is necessary for forming intimacy and establishing other values we regard as essential to being human, such as love, friendship, and trust.[4] Philosopher Dorota Mokrosinska argues privacy functions as a social good that citizens require to engage in a political democracy. Legal scholars Samuel Warren and Louis Brandeis argued privacy is the right to be let alone. One particularly useful definition of privacy comes from information scientist Helen Nissenbaum, who views privacy as contextual integrity: the appropriate flow of personal information. Because information technology enables pervasive surveillance, massive databases, and near-instant distribution of information across the globe—and because these technologies are able to know us better than we know ourselves[5]—she argues they present a new form of violation to our privacy that we need to address. Her solution is to understand our right to privacy as the right to live in a world in which our expectations about the flow of personal information are mostly met, where these expectations are shaped by social norms, with both local and general values, ends, and purposes (Nissenbaum 2010, 231).

[4] A common critique against such conceptions of privacy is that privacy is therefore not a useful stand-alone concept because almost all the time privacy could be swapped with another right which was infringed upon instead. This is the argument of Judith Jarvis Thomson, who argues we should dismiss the concept of privacy all together. But even if this were the case, privacy is still useful to us as a cluster concept—an accumulated value comprised through other values resembling each other. Analyzing privacy might require us to analyze privacy in particular contexts, but when shouldn't the context affect the analysis of profound, difficult to define but culturally cherished values such as privacy?

[5] This is because various technological innovations have made it possible to extract more information than ever before, and we often do not have access to this information. This is explained further in Part III.

Yet while this understanding of privacy seems to adequately address the information side of this process, this does not adequately address the transmission side of this process. It's not just about the context because there is something transformative about what we can do with our data.

Shoshana Zuboff coined the phrase "surveillance capitalism" in her book the *The Age of Surveillance Capitalism*. Under surveillance capitalism, our human experience is claimed as free raw material by corporations. These surveillance capitalists then use this material as a necessary resource in their commercial practices of extraction, prediction, and sales. This economic logic resulted in the realization that the best way to predict an outcome was to guarantee that outcome. This is the origin of instrumentarianism. Zuboff argues instrumentarianism is a new species of power: the power to know and shape human behavior toward other's ends (Zuboff 2019, 8). This power is realized through tools that—enabled by the loss of our privacy—grant others undue influence over us. Instrumentarian technologies are the tools at the heart of our surveillance capitalist economy, capable of modifying our thoughts and behaviors, often without our awareness. This complicates our autonomy to a potentially unsustainable level. It is through this new and unprecedented technology that our privacy is about more than the contextual integrity: privacy is not just about the appropriate flow of personal information, because this personal information is weaponized through transformative technologies to exert undue influence over us and disrupt our autonomy.

I argue we can better understand privacy as a cluster concept, best articulated through Daniel Solove's application of Ludwig Wittgenstein's framework for family resemblances. According to Wittgenstein, there does not exist an objectively true link between a word and the things to which it refers: there is no innate connection between the word and what it signifies. This means that while some concepts might not share a single trait, they still relate to each through "a

complicated network of similarities overlapping and crisscrossing: sometimes overall similarities, sometimes similarities of detail" (Wittgenstein 1921, 66). Like a web without a center point, a concept (family) may be comprised of other accumulated values (siblings) that resemble each other yet lack a singular analogous trait.

Solove advocates for a pragmatic approach to privacy: conceptualizing privacy from the bottom up, from particular contexts rather than getting stuck in the abstract. After reviewing previous conceptions of privacy, he finds them all either too broad or too narrow—a reoccurring problem for scholars trying to reconcile our desire for privacy in the wake of recent technological developments. By too narrow, he means definitions of privacy that are too rigid and unadaptable. By too broad, he means definitions of privacy that are too wide and all-encompassing. Instead, he wants to conceive of privacy by getting close to how we use with word 'privacy' without sacrificing logical consistency.

Instead of defining privacy by isolating core characteristics, we can instead understand privacy as drawing from a common pool of similar elements. According to Solove, the concept of privacy can be dealt with under six general headings: 1) the right to be let alone, 2) limited access to the self and the ability to shield oneself from unwanted access by others, 3) secrecy or the concealment of certain matters from others, 4) control over personal information and exercising control over personal information, 5) personhood and the protection of one's personality, individuality, and dignity, 6) intimacy and control over or limited access to one's intimate relationships or aspects of life (Solove 2002, 1009).

These headings are not perfect as there is significant overlap between them—and we still might wonder what exactly allows them to relate to one another. But we don't need perfection. Reflexive equilibrium—a philosophical methodology for justifying principles of inductive logic

developed by Nelson Goodman—holds that we can keep shifting our concepts and cases where those concepts are applicable, until they overlap one another. We might never be able to give a full account for sufficient conditions for privacy, but we don't need to: we may keep revising our theory of privacy as time goes on, and the concept of privacy can still prove useful. Classifying all the points in the web of privacy might yield categories with fuzzy boundaries that are in a constate state of flux, but we only need fixed and sharp boundaries for special purposes. Understanding privacy in this way still proves useful. This is especially true considering how advances in technology continuously unveils new quagmires that force us to reevaluate our moral systems and the virtues we uphold. A certain amount of malleability must be built into our definition of privacy. Solove's definition allows us to address the challenges instrumentarianism pose to our understanding of privacy.

Furthermore, the threat of instrumentarianism underscores what could be considered that particular thing which allows Solove's headings to resemble one another: privacy's special relationship to the growth and maintenance of our autonomy. This is because in each heading the violation of privacy implies a harm to our autonomy. While the tools of instrumentarianism appear to most explicitly align with his category of limited access to the self and the ability to shield oneself from unwanted access by others, instrumentarianism impacts each of his categories. This is because of privacy's fundamental role in our autonomy, which is precisely what tools of instrumentarianism exploit in order to access our autonomy.

I do not wish to say that this relationship is the only thing which makes privacy meaningful or distinctive. Even though privacy as protection from undue external influences is the most useful definition of privacy in the age of surveillance capitalism, it is important to recognize that this definition is not static—we simply don't know how future technologies will force us to revise this

new definition of privacy, just as the tools of instrumentarianism forced us to revise our old definition of privacy. Solove's framework for privacy includes this process of revision, and therefore avoids many of the technical challenges faced by privacy definitions which are either too broad or too narrow.

Due to the malleability Solove's conception of privacy entails, coupled with the fact that each of his headings is impacted by instrumentarianism, I argue that we can best understand privacy through his application of Wittgenstein's framework for family resemblances. And when we apply our modern of context surveillance capitalism and its tools of instrumentarianism (explained in Part III) to this framework, as well as the following investigations into how our privacy is necessary for our autonomy, I argue we can then define privacy as protection from undue external influences.

AUTONOMY AS EXPERIENCING OUR AUTHENTIC SELVES

Human autonomy is widely considered one of the most important values we hold. Although there are many illuminating accounts of autonomy, I will focus on the Kantian sense of autonomy, as it is one of the most influential accounts of autonomy in modern philosophy. Under this framework for autonomy, we are autonomous when our authentic selves are the source of the things we do.

In his early investigations into moral autonomy *Groundwork of the Metaphysics of Morals*, Immanuel Kant argues that what makes us agents is our capacity to find values in things. We create the sorts of things that are valuable in the world. To ascribe values, we require a certain degree of autonomy: for values to be considered mine in any meaningful sense, I as an agent must evaluate them and endorse them. What makes our values meaningful is that we ourselves chose them.

Values can't be chosen for us, nor can they be an unconscious, automatic reaction to some external stimuli. When we as agents exercise our capacity to find values in things—when we deliberate and decide whether or not to endorse our attitudes—we are experiencing our actions as coming from our authentic selves.

Christine Korsgaard, one of the leading Kantian scholars in modern philosophy, explains this process further. In *Self-Constitution*, she argues we can understand Kant's definition of autonomy in two ways: 1) that you are the source of your actions which come from you in the right sort of way, or 2) what matters is your endorsing things in the right sort of way, regardless of where they came from. Both ways of understanding Kant's definition of autonomy reiterate our role as agents: we can't just respond to the pushes and pulls of the world, but we must use our additional perspective as agents to evaluate those pushes and pulls. The "right sort of way" Korsgaard stresses are the conditions through which we experience our actions as coming from our authentic selves.

For Kant and Korsgaard, an authentic self is the achieved state of personhood after having evaluated and endorsed values for ourselves. When we do so, our authentic selves become the source of the things we do. This is important under Kantian ethics, because the capacity to decide for oneself and pursue a course of action is essential to the categorial imperative—which Kant viewed as the supreme guiding principle of morality. According to Korsgaard, this principle holds that we are morally required to see ourselves and the things that lead us to act as equal worth as other people's capacities to have values (Korsgaard 2009, 84). Human beings should be treated as an end in themselves and not as a means to an end. In other words, we are morally required to respect each other as agents just as we must respect ourselves as agents. This means respecting autonomy: allowing all individuals to be autonomous by experiencing their authentic selves as the source of the things they do.

PRIVACY AS A NECESSARY CONDITION FOR AUTONOMY

Claiming privacy as a necessary condition for autonomy isn't that controversial. Philosophical literature on privacy generally accepts that privacy plays a role in our autonomy—either by explicitly saying so or implicitly requiring such in its logical framework. Another reason why I chose to focus on Kantian autonomy is because this framework does not explicitly mention privacy, whereas the ethics I will be using later on do. Perhaps the reason why the relationship between privacy and autonomy has been undertheorized is because we've never had technology so capable of exploiting this relationship at such a global, inconspicuous scale. Most philosophers also agree that the technological developments in the last few decades have outpaced the general public's ability to understand how their privacy is compromised by them. Zuboff goes even further. She compares the introduction of instrumentarianism during the age of surveilliance capitalism to the introduction of totalitarianism during the world wars: in both cases, Western publics (especially the US) were genuinely unable to grasp the enormity of what was underway, "literally boggling minds" (Zuboff 2019, 356). Whereas totalitarianism was a political project that converged with economics to overwhelm society, "instrumentarianism is a market project that converges with the digital to achieve its own unique brand of social domination" (Zuboff 2019, 360).

With surveillance and instrumentarian technologies being so pervasive throughout our modern technological goods and services, it's important we clarify the relationship between privacy and autonomy. I argue the best way we can think of this relationship in the age of surveillance capitalism is understanding privacy as protection from undue external influence. Privacy is important for autonomy because if we are influenced in the wrong sort of way by our environment then our authentic self is compromised, and then we cannot be autonomous. Privacy

is what buffers against such negative environmental influences. Specifically, privacy helps keep us from being unduly influenced by others.

This is because privacy provides the time and space free from external pressures for us to decide what we want for ourselves. It is in these mental wilds where we're free to tinker with alternative thoughts or hone our shunned desires. Zuboff casts this space as sanctuary, noting how the Greek origins for this word as well as old English common law emphasize the link between sanctuary and "the unplunderable" (Zuboff, 2019, 478). Historically, sanctuaries have been viewed as fail-safes: guaranteed exits made available away from totalizing power, refuge found in another city, community, or religious place of worship. In a similar way can we view our mental wilds: as sanctuary, a fail-safe for our autonomy, a protective barrier to stop certain kinds of information or illicit influences from coming in. By safeguarding privacy, we ensure that we're free from inappropriate outside influences—influences which would otherwise compromise our autonomy by interfering with our ability to experience our authentic selves as the source of the things we do.

I argue that privacy is a necessary condition for the Kantian conception of autonomy. In both of Korsgaard's interpretations of Kant, privacy functions as that 'right sort of way' in which we are the source of our actions or endorse our actions. Consider how important it is for Kant that we as agents have the capacity to ascribe values in the world. For us to ascribe values—for us to have enough autonomy to meet the threshold of being an agent—we require privacy. After all, for values to be considered mine it must ultimately be me who chose them. In other words, I have to experience this choice as originating from my authentic self. It cannot come from my authentic self if this choice is made because of other undue external influences. Privacy serves as a necessary buffer against this. When we lose privacy, we lose that space to properly ascribe values. And if can't evaluate what's valuable or not, then nothing is valuable. This means that under a Kantian

conception of autonomy, not only would privacy be a necessary condition of autonomy, but it would become morally impermissible to waive our rights to privacy. For now, however, we can move forward having established that privacy is necessary for autonomy, and that we can best clarify this relationship as privacy protecting our autonomy from undue external influences.

Part II: Modern Personhood

A LIFE WORTH CHOOSING

One of the earliest and most influential concepts in moral philosophy is what Socrates called the "good life": the kind of life that is most worthy of a human being, the kind of life worth choosing from among all the different ways we might live (Vallor 2016, 2). For example, most would agree that a life full of fear and isolation is fundamentally less worth choosing over a life full of peace and friendship. Such a life might still have value, but since there are much better alternatives, that life would not be a life worth choosing.

In our modern age, the life worth choosing is a life of modern personhood. By modern personhood, I mean the sort of autonomous state achieved through certain standards of living our society appears to uphold as ideal. Employment, education, healthcare—these are so essential to the modern citizen that many characterize having adequate access to them as a human rights issue. I define these goods which modern citizens can reasonably expect to enjoy (and that they require to fulfill their modern personhood) as the goods of modern life. We send our children to school not because we demand them to choose this life, but because we view the goods of modern life as being so valuable that they at least have the right to initially enjoy them. Furthermore, because the goods of modern life are necessary to compete and thrive in our pursuit of modern personhood, we want to make sure our children start out with access to these goods.

My conception of modern personhood and the goods of modern life comes from the fact that there are certain basic needs human beings have in order to live a good life. These needs have been filled in many different ways throughout history, but in our modern world these needs are increasingly filled or facilitated by modern technological goods and services. The overwhelming

majority of U.S. employers now pay employees via direct deposit instead of cash or check—meaning you'll need a bank account, as well as an email and phone number to access that account. Using the internet has replaced using books from the library as the primary means of research for students, while health professionals now store our health records in databases instead of filing cabinets. Upcoming musicians can't afford to ignore streaming services or podcasting, while many artists rely on crowd-funding through sites like Patreon. If you want to stay in touch with friends or loved ones during the rolling lockdowns of the coronavirus pandemic, then you might rely on Zoom—a video communication software program that many schools, business, and governmental agencies used to continue functioning during lockdowns. Or perhaps you're among the 85% of U.S. adults who rely on their smartphone[6]—a device so integral to the daily lives of many that nearly half of adults reported that they "couldn't live without" them.[7]

To further clarify how we use modern technological goods and services to fulfill our modern personhood, I will explain how we rely on social media to fulfill our need for social connection in our modern time. Social media are interactive forms of media on the internet through which users publish and exchange content. Perhaps one of the most well-known goods of modern life is the degree to which we are now able to connect to one another across the globe through social media. Social media has revolutionized the way we organize, communicate, and express ourselves in modern life—so much so that "increasingly, no young person who wants a social life can afford not to be active" on social media (Zuboff 2019, 446). With approximately 72% of Americans using Facebook, Twitter, Instagram, or Snapchat, social media has become a vital tool for political engagement.[8] LinkedIn promises connections and opportunities professionals can't

[6] *Pew Research Center* 2021, "Mobile Fact Sheet"
[7] Anderson 2015, "6 facts about Americans and their smartphones"
[8] *Pew Research Center* 2021, "Social Media Fact Sheet"

afford to miss, while Tinder and Hinge are among various dating apps people use to find romantic relationships.

Grindr is a particularly interesting example. While gay men have always used subtle visual codes to identify each other in heteronormative cultures, the launch of Grindr in 2009 slowly pushed this identification online. Grindr is the largest geosocial app for queer folk, with almost four million daily active users worldwide (Tankovska 2021, para. 1). Regardless of whether Grindr acts as a positive force or a toxic[9] force in the lives of its users, its impact on gay culture and what it means to be a modern gay man is indisputable. For many gay men who want to meet other gay men for a date or casual sex, they need to be on Grindr. In homophobic regions in the US and abroad (such as countries like Jamaica and Uganda where homosexuality is illegal, or countries lacking LGBTQ+ protections like Russia and China), Grindr can function as the only safe and viable means for a gay man to communicate or arrange to meet other gay men. Others need Grindr because modern culture exerts intense pressure for them to have a presence on this app. Anecdotes about gay men scrolling on Grindr while at a dance club or on a date abound, but a better way to understand what's going on here is to think of Grindr as a vital tool that gay men require to compete and thrive in the economy of love—especially when they live in an area that's hostile to this type of love. To not participate in this app becomes a form of self-imposed celibacy. To be offline is to become invisible. Simply put, if you're gay and not on Grindr, you might hardly feel gay at all.

[9] For all of Grindr's benefits, Grindr is commodifying. You package yourself. You parse every bit of your flesh into digits, you brand yourself with labels called tribes. Though Grindr eventually launched a campaign called "Kindr" to quell the rampant racism, transphobia, fat-shaming, and bullying on the app, research continues to show that Grindr negatively impacts the mental health of its users, with common ailments being addiction, depression, and (ironically) isolation (Bloodworth 2018, para. 9).

My point in detailing the example of Grindr is to demonstrate how deep our dependency on social media for our basic need of social connection has become. Again, this isn't to say there aren't other ways to fulfill this need, but in our modern age social media is increasingly becoming a necessary way we do so. Depending on your identity, this need might run even deeper.[10] Aside from family and friends, our jobs might require us to use social media, in addition to certain schooling courses that require students to use social media (even if for just a project). Furthermore, the modern life our society appears to promote certainly includes the connection only social media can bring, whether that's being able to livestream a revolution or videocall a loved one on their deathbed.[11]

We use such modern technological goods and services to access the goods of modern life. Just as enjoying the goods of modern life in 1950s America entailed owning your own home and driving your own car, enjoying the goods of modern life today entails having access to social media. As one of the goods of modern life, social media helps us fulfill our modern personhood. Simply put, living a modern life as a modern person means accessing certain technological goods and services which enable or facilitate our modern existence. If we want to flourish in modern life, then we need the tools that help us do so. And though not everyone chooses this life worth choosing, the investment we put into our children (public schooling, children's health insurance programs) seems to suggest we at the very least want to enable our children to pursue this life.

---

[10] If identities have different degrees of reliance on technological goods and services, then some identities might be even more vulnerable to the coercive nature of our current social contract than others. While my Grindr example focuses on those identifying as gay men, other identities should also be analyzed in this way. Investigating how our modern technological goods and services might prevent marginalized peoples from meaningfully performing or developing their identities would be an extremely insightful project—but for now I will only note that such a threat of identity denial certainly warrants deeper analysis.

[11] Many did just this over the last year, as the coronavirus pandemic forced people to say their final goodbyes over videocalls due to quarantine.

And if that is the case, then we also must acknowledge that individuals require access to modern technological goods and services in this pursuit.

EUDAIMONIC & TECHNOMORAL VIRTUE ETHICS

Ethics can be broadly understood as reflective inquiry into the good life—the life worth choosing. Virtue ethics focuses on the role moral virtues play in achieving this good life. Moral virtues are the states or stable dispositions of a person's character, such as honesty or patience. According to virtue ethics, moral virtues should be actively cultivated and properly integrated through correct actions and practices, as they lead to deliberate, effective, and reasoned choices of the good. Reasoning is central to virtue ethics (holding that agents should always assess the context of a situation before expressing their virtues), but an agent's emotions, habits, and desires are just as important. In other words, a virtuous person not only thinks and acts appropriately, but also feels and wants appropriately. While Aristotle's *Nicomachean Ethics* is the most influential account of virtue in Western philosophy, other works from East and Southeast Asia also helped establish the field of virtue ethics. In ancient China, Kongzi (Latinized as Confucius) originated the moral philosophy known as Ruism, while on the Indian subcontinent Nepal-born Siddhārtha Gautama founded the religious and philosophical practice of Buddhism.

In assessing our technosocial contract I will be adopting eudaimonic virtue ethics as conceived by Lorraine Besser-Jones, with additional consideration to the technomoral virtue ethics as conceived by Shannon Vallor. I believe these moral frameworks are logically compelling and well-suited for this project. Eudaimonic virtue ethics reframes morality around our psychological well-being, while technomoral virtue ethics draws from Aristotelian, Confucian, and Buddhist

virtues to refocus morality on what is most likely to increase our chances of flourishing in our global technosocial conditions.

Besser-Jones advocates for our virtue ethics to be guided by the psychological conception of eudaimonic well-being, rather than the Aristotelian concept of eudaimonia. Thinking of virtue in instrumental terms, she restructures virtues in service of our innate psychological needs. She does this because empirical evidence shows that our innate psychological needs are just as vital for our psychological health as innate biological needs are vital for biological health, with researchers noting that "individuals cannot thrive without satisfying [innate psychological needs] any more than people can thrive with water but not food" (Besser-Jones 2017, 14). She also details how empirical research stresses that innate psychological needs are important and impactful for individuals regardless if they're conscious of them or not—what counts is having experiences which satisfy those needs. She identifies three innate psychological needs to model her virtues on: competence, relatedness, and autonomy.

Besser-Jones defines autonomy through her psychological conception of autonomy: the need to experience ourselves as the origin of our own behavior, to engage in activities we perceive to be our own and endorsed as our own. In other words, to experience ourselves as the source of the things we do. One of three good psychological states her virtues strive for is the development of certain cognitive structures that operate both as a regulatory feedback mechanism and as an aid to the actual implementation of individual goals—an important state for maintaining our autonomy. She argues that autonomous motivation (when agents perceive their goals as autonomously legislated) is much more productive than controlled motivation, where goals are imposed upon them (Besser-Jones 2017, 137). For this and many other reasons does Besser-Jones argue that acting virtuously entails acting in ways which foster our autonomy.

Another core commitment Besser-Jones adheres to during her work *Eudaimonic Ethics* is psychological realism. Psychological realism holds that moral theorizing ought to be conducted with a psychologically realistic picture of human nature. In this project, I too will adopt this commitment. If we're trying to figure out whether or not our technosocial contract is justified, we should stay mindful of how we can realistically expect people to react to this contract—specifically on their psychological reaction to the two choices our technosocial contract presents us: to enjoy modern personhood at the cost of your privacy or to not enjoy modern personhood at all.

I would also like to consider technomoral virtue ethics in my analysis of our technosocial contract. In her book *Technology and the Virtues*, Vallor admits that many contemporary scholars argue that Confucianism and Buddhism don't share any robust conceptual core with Aristotelian virtue ethics, but she counters that there are convincing arguments for why these three traditions do indeed share a conceptual core. One strategy she details is comparative philosopher Bryan Van Norden's thin/thick distinction for moral concepts. Thin concepts only give the essential structure of an idea, whereas thick concepts flesh out that idea in greater detail. Using this framework, Norden identifies at least four thin commitments shared by virtue ethics traditions, which Vallor summarizes as 1) a conception of the 'highest human good' or 'human flourishing', 2) a conception of moral virtues as cultivated states of character manifested by exemplary persons, 3) a conception of the practical path of moral self-cultivation, and 4) a conception of what human beings are generally like (Vallor 2016, 44). This is important because it allows a virtue ethic that is pluralistic (open to more than one mode of expression of human flourishing) and malleable (adapted to the needs of the present human condition and environment). Vallor also cites philosopher Alasdair MacIntyre in defense of virtue ethics. Although MacIntyre rejects the notion of extracting a single list of universal moral virtues from these diverse traditions, he believes they do share a conceptual

core. He argues a given reference to a virtue is only meaningful 1) within the context of a recognized human practice dedicated to securing moral goods internal to that practice, 2) where that practice is embedded in a coherent narrative concerning a whole human life, and 3) where that life is itself understood as participating in a shared moral tradition of seeking the highest good for a human being (Vallor 2016, 45).

While virtue ethics has fallen out of popularity over the centuries, Vallor makes a compelling case for why we should revisit them. She argues that "any contemporary theory of ethics—that is, a theory of what counts as a good life for human beings—must include an explicit conception of how to live well with technologies" (Vallor 2016, 3). Our moral practices have always been impacted by our technologies because our technologies alter our thoughts, behaviors, and judgement. Through technology, new possibilities for human action are born, while others are disabled or withheld—introducing new and complicated questions of morality. Vallor offers the example of how the introduction of bows and arrows gave humans the ability to kill more efficiently from farther away, therefore introducing new moral dilemmas of whether or not it was right or wrong for them to do so given a particular situation. Now with nuclear bombs, you can now instantly obliterate entire countries with relative ease. With genetic modification, you can alter your child before it's born. Vaccines save lives, but should they be mandatory? Automation makes production cheaper for businesses and prices cheaper for customers, but how do we choose who gets to be replaced by a machine and who doesn't? Again and again, we've seen new technologies give rise to new complications for those wishing to simply live a full and happy human life. This suggests that technology should indeed be explicitly addressed by modern ethics.

And though technology has always complicated morality, there is something truly new and unique about the power of modern technology. Vallor notes how never before has our

technological activity modified the very planetary conditions which makes life possible. This leads Vallor to argue that decisions in the 21st century about how to live well are not just moral decisions, but technomoral choices, "for they depend on the evolving affordances of the technological systems that we rely upon to support and mediate our lives in ways and to degrees never before witnessed" (Vallor 2016, 2). Our collective moral choices in technological contexts affect the well-being of other species, people across the globe, and generations not yet born. And it's increasingly unclear how much the future moral labor of our species will be performed by human individuals. For example, driverless cars make ethical choices during emergencies, while advanced AI-algorithms sort us as hireable or unhireable.

For Vallor, such a technological landscape complicates our ability to achieve the good life. Part of this is due to our acute technosocial opacity—what Vallor calls the paralyzing blindness created when one tries to account for all the complicated and diverging ways modern technology impacts our moral choices. This is precisely why Vallor argues virtue ethics are better positioned to address this dilemma. She argues the fixed rules and principles of other moral frameworks such as utilitarianism or Immanuel Kant's categorical imperative can't keep pace with all the uncertain paths of technosocial development we've witnessed and will continue to witness (Vallor 2016, 7). Virtue ethics, however, is malleable—in fact, an important feature of Vallor's proposed technomoral virtues is that they explicitly remain adjustable to our ever-shifting technological landscape.

Given this landscape, she frames her technomoral virtues around increasing our chances of flourishing in our global technosocial conditions. She identifies twelve virtues that do: honesty, self-control, humility, justice, courage, empathy, care, civility, flexibility, perspective, magnanimity, and technomoral wisdom. According to Vallor, our modern technological goods and

services have complicated our cultivation for each of these. Though I will be elaborating on this more later, what's important to note here is that her virtue ethic system presupposes the necessary, unavoidable role technology plays in our lives, as well as the complications they impose. This is not to say that modern technological goods and services—nor the goods of modern personhood which require us to access them—are incompatible with these virtues. The whole point of Vallor's project is to clarify how we *should* be using modern technological goods and services to cultivate these virtues. For example, technomoral wisdom is the most important of Vallor's technomoral virtues. Technomoral wisdom refers to the general condition of well-cultivated and integrated moral expertise that expresses all other virtues of character that we need in order to live well with emerging technologies. In order to cultivate technomoral wisdom, one would clearly need access to the emerging technologies they're supposed to using virtuously (i.e. practicing technomoral wisdom). While certain goods of modern personhood such as social media might sometimes conflict with cultivating technomoral wisdom, this doesn't mean social media is incompatible with our virtues: it just means we should 1) continue cultivating technomoral wisdom so we can make ourselves aware of how to use such goods without going against our virtues and 2) look into changing how we regulate or design our modern technological goods and services so that they better reflect our virtues.

CULTIVATING VIRTUES THROUGH THE GOODS OF MODERN LIFE

From healthcare to education, from social media to employment—the goods of modern life are those goods and services which modern citizens are expected to benefit from. When we use these goods and services, they help us fulfill our modern personhood, help us function as

autonomous individuals in our modern era. And according to eudaimonic and technomoral virtue ethics, access to the goods of modern life is an important part of cultivating our virtues.

Under eudaimonic virtue ethics, living virtuously means respecting and fulfilling our innate psychological needs: autonomy, competency, and relatedness. In our modern era, each of these are virtues are often fulfilled through the goods of modern life—which are increasingly facilitated through modern technological goods and services. Similar to how modern technological goods and services enable us to enjoy the goods of modern life, so do the goods of modern life enable us to fulfill our virtue of autonomy. Having good health thanks to adequate health care, gaining knowledge and skills through education, earning a living wage through employment—all of these goods grant more agency to the individual enjoying them. By this, I mean that an individual is generally able to live much more autonomously when they're enjoying these goods. Likewise, the virtue of relatedness (experiencing connections with others) is benefited by goods such as social media, and the virtue of competence (exercising one's skills in a way that contributes to one's society) is benefitted by goods such as the internet. That's not to say that there aren't other ways to fulfill these virtues, but that such goods of modern life are increasingly if not already the primary ways we do so.

Under technomoral virtue ethics, living virtuously means living in a way most likely to increase our chances of flourishing in our global technosocial conditions. It is worth noting that technomoral virtue ethics presupposes that we as modern humans will necessarily be engaging with modern technological goods and services, and that we therefore will need to cultivate our virtues partially through modern technological goods and services. But I argue that the goods of life themselves also help us cultivate these virtues. After all, the whole point of Vallor's project is to articulate the proper way to use technology in order to cultivate technomoral virtues. Consider

again the case of Grindr. It might seem odd to claim that accessing Grindr constitutes living virtuously. Indeed, there might be conflict between the life we have through Grindr and living a virtuous life—but again, that's Vallor point: there are myriad ways modern technological goods and services complicate our ability to live virtuously. We might use Grindr in the wrong sort of way, but that doesn't mean that this tool couldn't be used in a way to cultivate our technomoral virtues. As Vallor writes, "Why not demand useful tools that do not debilitate us?" (Vallor 2016, 169). In other words, modern technological goods and services have positive effects and negative effects on our ability to live virtuously—why deprive ourselves of the positives if can work on removing the negatives? In this example, it's not that gay men require Grindr to be virtuous, but it could very well be the case that they require something to fill the role of Grindr (perhaps another dating app) in order to live virtuously. After all, it seems unsatisfying to try and develop the virtue of care—defined by Vallor as "a skillful, attentive, responsible, and emotionally responsive disposition to personally meet the needs of those with whom we share our technosocial environment"—if you're not even allowed to pursue a meaningful romantic relationship, let alone communicate with someone of your own sexual identity.

Considering the role of goods of modern life serve in our cultivation of eudaimonic and technomoral virtues, it would seem morally impermissible to decline the goods of modern life. This is because total withdrawal from modern technological goods and services is incompatible with cultivating our virtues, in the sense that to go without such tools is to needlessly obstruct our ability to live virtuously. Specifically, because modern society requires us to use modern technological goods and services to participate in various facets of society, clicking disagree would severely hinder our ability to function autonomously. By this, I mean opting out of modern technological goods and services would effectively restrict our freedom to the point of hindering

our ability to experience ourselves as the source of the things we do. After all, it's difficult to feel like the source of the things you do if the vast majority of the things you'd want to do in modern society is locked away from you. To be denied the goods of modern life (to lose access to modern technological goods and services) is to then deny modern personhood. Aside from the material loss of modern personhood (the myriad benefits spawning from goods such as but not limited to healthcare, education, and social media), when one considers how Vallor's technomoral virtue ethics hinges on the fact that humanity's modern technology is so impactful that we must reorient our entire ethics in reckoning of this technology, then surely to be denied to partake in said technology is to be denied being treated as human, as autonomous, as a modern individual of equal moral consideration.

Losing the ability to cultivate our eudaimonic and technomoral virtues becomes a violation of one's rights because denying these virtues entails denying the fulfillment of basic human needs—needs that we increasingly fulfill through modern technological goods and services. By cultivating eudaimonic and technomoral virtues through these goods and services, we fulfill our modern personhood and enjoy goods we as modern citizens know ourselves worthy of enjoying, such as education, healthcare, and social media. Recalling the example of Grindr, to deny a queer individual access to this service might constitute denying them the only safe way to love and therefore fulfill their authentic selves. And keeping to our commitment to psychological realism, it would be psychologically unrealistic for your average queer person to view the expulsion from modern personhood (including such a service as Grindr) as anything but a harm, and for most a particularly unbearable one at that.

Part III: Instrumentarianism

SURVIELLANCE CAPITALISM & ITS HARMS

Modern technological goods and services operate under an exploitative, harmful economic order best understood as surveillance capitalism. This system profoundly diminishes our privacy, allowing others access to our autonomy through instrumentarianism. While many harms of surveillance capitalism are generally known by the public and discussed by scholars across disciplines, they haven't necessarily discussed these harms in relation to our autonomy. But because instrumentarian tools modify our thoughts and behaviors (often without our awareness), we need to. I argue that it is through these tools that our mental wilds are cut away and our autonomy becomes vulnerable. This directly contradicts eudaimonic and technomoral virtue ethics. Having our autonomy disrupted and made vulnerable in such a way is to endure an intolerable harm.

Zuboff provides eight definitions for surveillance capitalism. For the purposes of investigating our technosocial contract, I've merged five of them together to provide a basic definition of surveillance capitalism:

> As the foundational framework of a surveillance economy, surveillance capitalism is the new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales. This parasitic economic logic subordinates the productions of goods and services in favor of a new global architecture of behavior modification: this is the origin of instrumentarianism.

Surveillance can be broadly understood as close and sustained observation over someone or something. This process involves a transfer of information, where the person or thing surveilling

learns information about the person or thing surveilled—in other words, on information going out. One of the most well-known examples of surveillance technology is the panopticon. Originally conceived by Jeremy Bentham, the panopticon was an architectural design for prison: from the view of a single tower, guards could peer into each prisoner's cell. As a prisoner this meant you could be watched at any moment, but you never knew when. Bentham originally designed the panopticon as a tool for moral improvement—but Michel Foucault argues in his book *Discipline & Punish: The Birth of the Prison* that the panopticon also functions as a tool of social control: a subtle, persuasive, and coercive technology of people which we would now refer to as behavior modification technology.

Surveillance technologies have advanced far beyond the sort of surveillance described by the panopticon. This is because various technological innovations have made it possible to extract more information through surveillance than ever before. These developments are generally understood in three ways: 1) as powerful improvements in existing technologies[12] which therefore improve the quality of information extracted, 2) as the massive expansion of digital technologies[13] across the globe through which surveillance technologies may be applied, and 3) as developments in the ability store and process extracted information. This includes our increasingly powerful and opaque tools of analysis. These third type of innovations are the technologies that I and others refer to when we talk about others knowing more about us than we know ourselves. This usually involves analyzing metadata—data about data sets. For example, modeling involves the analysis

[12] For example, advances in digital photography make it possible to read and even clone fingerprints from photos only showing parts of someone's hands (Wood 2018, para. 21).

[13] Such technologies are becoming increasingly invisible in the world around us. As Google CEO Eric Schmidt acknowledges, the most profound technologies are those that disappear—that weave themselves into the fabric of everyday life so they are indistinguishable from it, allowing devices like computers to vanish into the background (Zuboff 2019, 98).

of aggregated data sets and generates information about people beyond what is given in the induvial data sets. “Likes” on Facebook are sufficient to accurately predict sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender—a stunning tool that is able to identify psychological traits “as accurately as a psychologist administering a standardized, validated instrument” (Tufekci 2014, para. 35). Meanwhile, researchers using facial recognition technology concluded that deep neural networks could detect sexual orientation from faces with around 80% accuracy—besting the judgement of humans (Wang and Kosinski 2017, 2).[14] And thanks to advances in DNA analysis and popular commercial practices that collect biometric information, individuals disclosing their genetic information also disclose the genetic data of their family members, past and present. This is particularly worrying as it is not only impossible for those not yet born to consent to their genetic data being extracted, but it could be potentially damaging for such information to be known by potential employers or others who might use this information against them.

The introduction of instrumentarian tools further encouraged developments of this third type, with new methods such as affective computing, emotion analytics, and sentiment analysis being created to render both our conscious and unconscious emotion as observable behavior. Affective computing refers to systems and devices that recognize, interpret, process, and simulate human affects. Emotion and sentiment analytics use data about a person’s verbal or nonverbal communication to learn their mood or attitude. All three entail sensitive information and personal

[14] This technology poses a massive and immediate threat to queer individuals across the globe, specifically in areas where being queer is outlawed and punishable by death.

data one otherwise might not broadcast being derived from seemingly innocuous bits of data, such as but not limited to tweets, selfies, and the tone of our voice.

In America, concerns over surveillance are traditionally concerns over government surveillance. An interesting contrast can be found in China. While the Chinese government controls its surveillance technologies and instrumentarian tools, corporations are the ones who control these in America and in much of the Western world. This doesn't mean American citizens are any better off when it comes this imbalance of power, as Zuboff writes: "No other time in history have private corporations of unprecedented wealth and power enjoyed the free exercise of economies of action supported by a pervasive global architecture of ubiquitous computational knowledge and control constructed and maintained by the advanced scientific know-how that money can buy" (Zuboff 2019, 308). The degree to which corporations surveil us has only recently breached public awareness. Zuboff credits the dawn of surveillance capitalism to America's reaction to the terrorist attacks of 9/11 and the neoliberal policies advanced between Google and intelligence agencies.[15] Specifically, she pinpoints Google's invention of targeted advertising for not only paving the way to Google's financial success and current technological dominance, but as the origin point for the economic imperative that our personal data be rendered as raw material for hidden practices of prediction, sales, and influence. These events created a doctrine she calls surveillance exceptionalism, which can roughly be understood as the political belief that surveillance for the sake of safety is not only acceptable, but the correct thing to do in response to

[15] Following the events of 9/11 politicians quickly passed the Patriot Act, which among other things diluted judicial oversight in invading the privacy of civilians. Additionally, the US government went on to advocate for the intentional inclusion of exploits into American technology and infrastructure, just for the sake of surveillance—despite the fact these exploits could also be used by hackers or other nefarious actors (Snowden 2019, 194). In fact, CIA Director Hayden admitted that during the years following 9/11 America could be fairly charged with the militarization of the world wide web (Zuboff 2019, 114).

threats such as terrorism. What followed was a mutually beneficial arrangement: user data gave corporations vast profits, and the government could pilfer this data for free. This collaboration between Google and the NSA was unprecedented. As time went on, the gap between privacy protections against surveillance by the governmental and privacy protections against surveillance by corporations only widened. Surveillance capitalists (those profiting off the sale of our extracted information or by selling access to us through instrumentarian tools) engineered sophisticated multi-state-level lobbying campaigns to fight back against any proposed legislation that would augment our privacy or curtail their behavioral data surplus operations.

All of these converging technological developments that constitute surveillance capitalism and its new instrumentarian power warrant more examination than I will pursue for my analysis of our technosocial contract, but here I shall briefly clarify the general process of how surveillance capitalism operates:

1) When we engage with modern technological goods and services, our human experiences are claimed as free raw material by corporations. By human experiences, I'm referring to the personal data created when we interact with these technologies, such as one's location, the contents of an email or text, or audio and visual recordings both passively and actively collected by our devices. Various converging technological innovations have amplified the quantity and quality of information that can be extracted from this material. More surveillance means more data, and more data means more material—this created the extraction imperative, which holds that raw-material supplies must be procured at an ever-expanding scale.
2) These materials are fed through machine intelligence technologies which translate into behavioral data surplus. Such technologies are currently kept as corporate trade secrets.

Behavioral data surplus refers to information not related to the use of a product or service that is then used to predict the future behavior of the person this data is extracted from. Corporations use this data to improve their tools of instrumentarianism—such as Facebook using this data to train their facial recognition technology and Google using this data to train their AI.[16] These instrumentarian tools are also kept as corporate trade secrets by tech companies. Additionally, they use this behavioral surplus data to produce prediction products designed to forecast what we will feel, think, and do in the future, and then sell these prediction products to advertisers and other interested third parties on behavioral future markets. Under surveillance capitalism, selling these prediction products (aided by instrumentarian tools) is far more lucrative than selling goods or services to customers.

3) Better predictions mean more profits—this created the prediction imperative, the realization that the best way to predict an outcome was to guarantee that outcome. This led to aggressive economies of scope and action. Economies of scope refers to operations pushing beyond the virtual world in order to mine behavioral surplus data from the "real" world (such as devices unnecessarily installed[17] with Wi-Fi and

[16] Google's machine intelligence capabilities feed on behavioral surplus, and the more surplus they consume, the more accurate their prediction result. This leads some such as investigative reporter Kevin Kelly to conclude that "it's more likely that Google develops Search as a means of continuously training its evolving AI capabilities" (Zuboff 2019, 95).

[17] Devices like smartphones, smart TVs, smart fridges—the use of "smart" here is just one example in a long history of corporations attempting to rebrand surveillance in a positive light. Addiction to screens is labelled "user engagement" while techniques designed to tamper with your unique mind is called "personalization"—as Véliz writes: "Tech has gone so far in seducing us through words that it has even sequestered the language of nature … you used to be able to taste the sweetness of an apple, listen to bird tweet at sunrise, wade your feet into a stream, and find shapes in the clouds passing by … now these words are mostly used to describe things that are the opposite of nature" (Véliz 2020, 64).

> analytics focused on uncovering intimate patterns of the self). In other words, this imperative creates an economic logic to maximize the territory (physical or mental) which can be surveilled. Economies of action refers to the tools of instrumentarianism: technologies designed to intervene and shape our behavior in order to better their own predictions. In other words, this imperative creates an economic logic which views autonomy (protected by our privacy) as a threat to profits.[18] For surveillance capitalism, our ability to resist its undue influence is unacceptable.

But before I elaborate further on the tools of instrumentarianism and how this threatens our autonomy, I want to describe some of the general harms produced by surveillance capitalism.

It's first worth clarifying how surveillance technologies functioning under surveillance capitalism generally harm our privacy and autonomy. For example, one might wonder how surveillance technologies could impact our autonomy if we're unaware we're being surveilled and therefore unaware our privacy is being invaded. The reason why our autonomy is still diminished in such a case is because surveillance involves a transfer of information: the observer learns something about the observed. Even in the case where the observed is a person walking down the street and the observer is a security camera, the security camera receives information about the person walking by—the person's privacy is reduced as the security camera records information about them, information which can then be used to exert undue influence over their autonomy. In

---

[18]Although surveillance capitalists often claim objectivity and neutrality when using tools of instrumentarianism, research shows that manipulations to algorithms by Facebook and Google continue to reflect corporate commercial objectives—as legal scholar Frank Pasquale describes it: "The power to include, exclude, and rank is the power to ensure which public impressions become permanent and which remain fleeting … They help create the world they claim to merely 'show' us" (Pasquale 2015, 60).

other words, surveillance technologies inevitably impact our autonomy because privacy is a necessary condition for autonomy.

Another important clarification regarding surveillance capitalism and its general harms to our privacy and autonomy is how the attainment of data farmed from an open source or public venue can still constitute an invasion of privacy and threat to autonomy. Reconsider the security camera and the person walking down the street—at first glance, it might seem unreasonable to claim that the security camera is invading the person's privacy since the person is out in public. One might argue that personal data collected in such spaces isn't problematic because this data appears to be freely given, and there is also a limit to how much personal data can be expected to remain private when participating in such spaces.

Yet there are many ways surveillance capitalism complicates this scenario. It should be recalled that the surveillance technologies deployed across our public venues are now capable of extracting information which we justifiably expect to remain private, even in public venues. For example, if the security camera in this scenario is equipped with the appropriate AI-facial recognition software, then the security camera could determine the sexuality of the person walking down the street. Although there are many ways for someone's sexuality to become known, merely showing one's face in public shouldn't be one of them; security cameras learning the sexualities of passersby would appear to constitute an invasion of privacy.

Furthermore, considering our new definition of privacy—privacy as protection from external influences—then the collection of personal data from open sources qualifies as a problematic breach of privacy. The tools of instrumentarianism which allow others to access our autonomy directly relies on our personal data, including personal data available through open sources. We might not object to someone googling their classmate to learn what they can about

them, but we would object to someone surveilling their classmate to the degree our modern technological goods and services surveil us. Recall how recent technological innovations have created the ability to extract new information by analyzing metadata. If someone was using these tools of analysis to extract new and profound personal data from existing personal data about their classmate online, then (thanks to the tools of instrumentarianism) they're also extracting the resources to exert undue influence over them. Because instrumentarianism grants others access to our autonomy—and because this access is achieved through the loss of our privacy—then the attainment of such data remains problematic, even when this data originally derives from an open source.

There are many harms to such a system, but there are two ways surveillance capitalism proves exploitative that I wish to highlight. The first way surveillance capitalism appears exploitative to potentially intolerable degrees is what Zuboff refers to as the unauthorized privatization of the division of learning. She argues that surveillance capitalism shifted the ordering principle of the workplace from a division of labor to a division of learning—we conquer new intellectual skills and learn to thrive in our information-rich environments, but there's deep conflicts of knowledge, authority, and power (Zuboff 2019, 180). One way to understand these conflicts is through problem of two texts. There are the public facing texts (our screens) which we're the authors and readers of, and then there's the shadow text (what's behind our screens)—a burgeoning accumulation of behavioral surplus and its analyses which says more about us than we know about ourselves. This shadow text automatically feeds on our experience as we engage in the normal and necessary routines of social participation. This a severe asymmetry in knowledge—after all, those who are surveilled (customers, citizens, students and teachers, employees) are excluded from the opportunity to benefit from the knowledge found in this shadow text and lack

any means within this distribution of learning to challenge this asymmetry. Another way to understand this asymmetry of knowledge is to understand that knowledge is a form of power. Other philosophers have discussed surveillance capitalism in these terms—the thesis of Véliz's book is that privacy functions as a form of power, and that the ability to forecast and influence people based off their personal data is "the quintessential kind of power" in the digital age (Véliz 2020, 53). Drawing from Michel Foucault's theories on how there is power in knowing and knowledge in power[19], Véliz points out that power constructs human subjects, saying: "The more someone knows about us, the more they anticipate our every move, as well as influence us … power generates certain mentalities, it transforms sensitives, it brings about ways of being in the world" (Véliz 2020, 52). And if knowledge (and privacy) is power, then surveillance capitalists are extracting the most potent and distilled form of this power: intimate knowledge about yourself that you yourself are unaware of. For example, if you're uncertain about your religious beliefs, sexual orientation, or political leaning—chances are your consumer profile is certain. And while it might be fine for more to be known about you than you know about yourself, it doesn't seem fine for corporations to hunt, extract, and commodify this information—let alone immediately weaponize it against you by trying to exert undue influence over you through tools of instrumentarianism. The fact that surveillance capitalism forces us to relinquish such power in order to access the goods and services we need just to function as modern citizens is exploitative to a degree we can justifiably view as unacceptable.

[19] Indeed, according to Foucault, "We must cease once and for all to describe the effects of power in negative terms: it 'excludes', it 'represses', it 'censors', it 'abstracts', it 'masks', it 'conceals'. In fact, power produces; it produces reality; it produces domains of objects and rituals of truth. The individual and the knowledge that may be gained of him belong to this production" (Foucault 1995, 194).

The other way surveillance capitalism is exploitative that I want to highlight is how this system amounts to outright theft. This theft can be thought of as digital dispossession, the seizure of our human experience as material for surveillance capitalism's market mechanisms—Zuboff credits this original act of seizure as the originating point for surveillance capitalism (Zuboff 2019, 99). What results is a profound disruption in the historical consumer and product dynamic. Because corporations make more money selling access to us, it is more accurate to refer to advertisers and other actors purchasing this access as the actual customers, while we are more like something farmed. The 'product' of value in this exchange is the behavioral data surplus that is ripped from our lives. As Zuboff phrases it, "You are not the product, you are the abandoned carcass" (Zuboff 2019, 377). Furthermore, this has severe repercussions for society as we know it. Whereas before capitalism's cycle of supply and demand catered to the genuine needs of populations and societies and enabled the fruitful expansion of market democracy, surveillance capitalism no longer has any direct connection or interest in the needs of populations, societies, or states. This shift is extremely worrying and underscores the degree to which surveillance capitalism has rewritten the rules of our society.

Of the many harms surveillance capitalism produces, there are myriad material harms we endure through our diminished privacy. By material harms, I refer to harms which seem unobjectively harmful to an individual's ability to function in modern society. For example, in her book *Weapons of Math Destruction*, Cathy O'Neil details the proliferation of problematic mathematical machine-powered models which increasingly manage our lives. These predictive models often encode human prejudice, misunderstanding, and bias into their software (O'Neil 2016, 3). They also require our privacy (our personal data) to function, and are everywhere in fields such as human resources, healthcare, and banking. These digital models produce tangible

harms. For example, a growing number of employers use wellness programs to surveil employees via health devices such as Fitbits and Apple Watches. After processing their personal data, an employee's health insurance premium goes up or down (O'Neil 2016, 175). Similarly, it is common practice for employers to demand a potential employee's credit card data before hiring them. This is thought to weed out individuals who are unscrupulous or untrustworthy—but this also acts as a dangerous poverty cycle (O'Neill 2016, 148). After all, how can one climb out of debt if they can't earn the funds to do so? In other cases, an employer may not hire you because their models have discovered you have a mental illness based on how you answered their survey (O'Neil 2016, 106).[20] Meanwhile, these models help ads pinpoint people in great need to sell them false or overpriced promises. For example, in training materials for recruiters at Vatterott College, they were explicit about preying upon those in pain, with one slide depicting "an image of a dentist bearing down on a patient in agony, with the words: Find Out Where Their Pain Is" (O'Neill 2016, 73). The point of this message and image (and the whole presentation) was to emphasize how recruiters need to find prospective students' psychological vulnerabilities (their "pain") in order to better lure them into attending Vatterott College.

Another material harm worth noting is the perpetuation of inequality. As previous mentioned, some of these new technologies unintentionally encode human prejudice, misunderstanding, and bias into their software systems. One way this manifests is through predictive policing. Through predictive policing, officers use surveillance and data-mining tools to predict and preempt criminal activity. This is especially worrying, as racial bias within the

[20] As O'Neil writes: "Consider the feedback loop that the Kronos personality test engenders … red-lighting people with certain mental health issues prevents them from having a normal job and leading a normal life, further isolating them ... this is exactly what the Americans with Disabilities Act is supposed to prevent" (O'Neil 2016, 112).

American criminal justice system is a well-known problem. In fact, Simone Browne argues in her book *Dark Matters* that surveillance has always been used to reinforce racial hierarchies in the US by regulating blackness. Considering how developing technologies continue to be racially designed we are right to worry about tactics such as preemptive policing.[21] Also referred to as "predictive policing", this practice involves advanced algorithms trying to predict potential crimes, victims, and offenders based on previous data. In theory this enhances public safety, but in effect this reinforces institutional biases. This is partially due to biased data being fed into these algorithms which then produces biased outcomes. According to various studies, such predictive policing systems exacerbate racial discrimination in our criminal justice system (Crawford et al 2019, 193).

We are also right to worry about how our modern technological goods and services disproportionately levy harms against minority identities, and how at the very least surveillance capitalism provides tools ripe to exploit and harm minority identities. Another way to understand the fundamental inequality imposed by this system is through how personal data operates. In fact, this leads Véliz to view privacy as justice's blindfold: that which blinds the system to ensure we are all treated equally. As she writes:

> The very essence of the personal data economy is that we are all treated differently, according to our data. It is because we are treated differently that algorithms end up being sexist and racist … it is because we are treated differently on account of our data that

[21]As Snowden quips: "No policing algorithm would ever be programmed, even if it could be, toward leniency or forgiveness …. A world in which every law is always enforced would be a world in which everyone was criminal," (Snowden 2019, 197). I agree with Snowden in that, in addition to the problematic convergence of racist policing practices and powerful surveillance technologies, there seems something fundamentally intolerable about every law being automatically enforced. It could be said that there is a certain beauty in slight, non-harming acts of deviancy—perhaps a flash of wild.

> different people get to pay different prices for the same product without knowing they might be paying more than others. It is because we are treated differently that we get to see different content, which further amplifies our differences—a vicious cycle of otherness and inequality. No matter who you are, you should have the same access to information and opportunities (p. 86).

Véliz goes on to argue that personal data is so toxic that we should ban the trade in it altogether, just as we ban other trades (the buying and selling of people, votes, organs, etc.) we deem too harmful to be legal. Indeed, there does seem to be certain types of knowledge that we would find inherently wrong for someone to profit off of; it strikes us as gross and unethical for someone to profit off the knowledge that someone's loved one just died in a car accident. She makes a convincing case for this in her book, but for the purposes of investigating our technosocial contract we can for now just acknowledge that surveillance capitalism perpetuates discrimination and inequality in a way we have good reason to worry about.

Another worry many have with surveillance capitalism is its apparent threat to democracy. This is traditionally understood in two ways: 1) destabilizing the autonomy of citizens and 2) further bolstering corporation's power over democratic governments. As previously discussed, privacy is necessary for autonomy. Autonomy is widely accepted as a necessary component to democracy: any self-governing polity depends on individuals having autonomy, otherwise it's not meaningfully self-governed. This has led philosophers such Dorota Mokrosinska to argue that privacy serves as a social good: we are collectively interested in each other's privacy just as we are collectively interested in each other's autonomy. A good example of this is psycho-political metamorphosis. This is the term for Jeffrey Reiman gives for how our modern technological infrastructure problematizes our political autonomy: when we're surveilled like this, this stunts not

only our actions but how we reason, pushing us towards conventionally or a "happy medium" rather than thoughts that go against acceptable political thinking (Nissenbaum 2010, 76). Reiman regards our modern technological infrastructure as an informational panopticon. He reimagines Bentham's panoptic prison as a fishbowl, where people are visible from a single point. He argues this produces risks of extrinsic and intrinsic losses of freedom, as well as risks to our political autonomy. Consider self-censorship. Self-censorship isn't inherently bad, but it's worrying when people self-censor in ways that damage their autonomy. As Véliz writes, "When you don't search for a term for fear of how others might use that information about you, your autonomy and freedom are being limited" (Véliz 2020, 72). We might not care if the term being searched is something we wouldn't want someone searching in the first place, such as child pornography. But when googling becomes a means to form identity—perhaps a user is researching about different sexualities, political views, or religious convictions—then we do care if someone can search these terms without the looming threat of negative repercussions preventing them from doing so. Especially if they're googling alternative political thinking.

Furthermore, because instrumentarianism uses our diminished privacy to disrupt our autonomy, we have reason to worry that instrumentarian tools could be used to influence people to vote not because of their deepest convictions but because these tools manipulated their perceptions and beliefs. Political campaigns have always targeted key voters and tried to persuade them to their side, just as politicians have always presented themselves differently depending on who they're speaking to.[22] What is new and concerning about these tactics now is that our modern technological infrastructure might push these practices too far. For example, an important feature

[22] Common and often humorous examples of this are when politicians adopt different accents depending on which region of the country they're visiting.

of democracy is the ability for two opposing sides to agree on a basic set of facts that they can debate from. When political messaging and campaigns use tools of instrumentarianism, they are violating the spirit of our democracy: we want politicians portraying the same thing to all prospective voters, because this not only helps promote coherent debates between those of opposing sides, but it helps hold politicians accountable. The worry here is that surveillance capitalism will continue to worsen the inability for two opposing sides to share a common reality, and that instrumentarian tools could potentially manipulate a voter's views of a politician such that they are voting for or against someone based on a totally inaccurate understanding of them. Again, this isn't necessarily new, but what is new is the degree to which instrumentarian tools perfect this practice. In other words, we accept that a certain amount of persuasion is okay for politicians to engage in, but instrumentarianism might push this persuasion into outright manipulation.

The other way surveillance capitalism threatens democracy is through worsening the ever-growing imbalance between governmental and corporate power. According to Zuboff, surveillance capitalism rose to dominance in the US during conditions of relative lawlessness—meaning little to no regulation existed to curtail corporate practices such as claiming our human experience as free raw material for commercial ends or implementing tools of instrumentarianism throughout our digital economy. Furthermore, the organic reciprocity that exists in relationships between people as either consumers or employees is lost in this exchange; again, we are more like something harvested from. This is simply not the sort of relationship we want between the union of market capitalism and democracy because this prioritizes the needs of advertisers and other third-party actors (the actual customers in this exchange) over the needs of citizens (those harvested from). It is worth noting that in 2016 almost half of all donations to both political parties ($176 million) came from a small group of wealthy individuals and their corporations (Zuboff

2019, 43). Google and other surveillance capitalist corporations like Facebook lead aggressive lobbying campaigns against any efforts to regulate their practices or diminish their access to our personal data. Then add to this the fact that surveillance capitalists control the accumulation and processing of information about our behavior—and that we remain in the dark about the processes through which they understand our behavior as well as the exact knowledge gained in doing so—then we have good reason to worry that surveillance capitalism will only bolster corporate power over governments.

As Véliz puts it, "Having one of the most powerful corporations in the world know so much about us and allowing it to show us messages that can influence our voting behavior during elections is insane" (Véliz 2020, 105). It is insane because the rule of law cannot rely on good faith alone. We currently lack meaningful checks and balances against corporations doing the sorts of things we don't want them to do (such as deploying instrumentarian tools to manipulate voting outcomes). Our autonomy, as well as our democracy, should not be something we can only just trust that corporations will protect and not exploit.[23] We don't want corporations monopolizing public utilities like water and electricity—the same can be said for social media and other modern technological goods and services. We don't want corporations monopolizing our means of social connection. Currently, corporations monopolize what is becoming an increasingly popular language: emojis. Emojis (short for emoticon) are visual representations of emotions, objects, or symbols used across digital mediums. Not only are they extremely popular (now even appearing in news headlines and political announcements) but some have speculated whether a future global language would come from emojis: many "words" such as a smiley face have multi-lingual aspects

[23] Indeed, if corporations' handling of our natural wilds is any indication, then we have good reason to believe they will not only fail to protect our mental wilds but actively cause their destruction.

to them, rendering them comprehensible across languages. So far, the Oxford Dictionary named the "Face with Tears of Joy" emoji as the Word of the Year for 2015, while some studies estimate that more than 90% of users social networking communicate with emojis (Zareen et al 2016, 257). If emojis continue to grow in popularity or do indeed become a useful global language, then we should worry about corporations retaining complete control over this language; a language is something we shouldn't want corporations monopolizing. Whereas before words were something defined and revised by people over time, now it is corporations who we rely on to define and revise this language. We have no means to tweak emojis, let alone upload our own to use. If a government prevented citizens from revising, creating, or using words of their own design in this way, we would call this government totalitarian. Likewise, we should regard corporations monopolizing an entire branch of language with equal scrutiny.

The final harm I want to touch upon is the profound impact modern technological goods and services appear to have on our mental health—notably on the mental health of younger generations. First and foremost, it's worth recalling a major point in eudaimonic ethics: that our innate psychological needs are as vital to our psychological health as our biological needs are vital to our biological health. Autonomy is one of our most important psychological needs. Because interacting with modern technological goods and services necessarily diminishes our privacy and features instrumentarian tools that use this decline in our privacy to disrupt our autonomy, it is perhaps understandable why we're seeing such poor mental health from those that interact with modern technological goods and services the most. Especially if we recall how Besser-Jones stresses that empirical research shows that matters is if we're having autonomous experiences or not, regardless of if we're conscious of having them or not. In this sense, we could be thinking we're acting autonomously when engaging with a specific instrumentarian tool, but if we're not

actually functioning autonomously enough in this exchange, then we won't actually be fulfilling our psychological need for autonomy.

A good example of such a tool are smartphones. 95% of Generation Z use smartphones, and a similar amount use social media (Watson 2018, para. 2). For better or worse, smartphones are iconic of not only our modern age but also of millennials and Gen Z: they use them the most, and they are the first generations who used them during their formative years of childhood, adolescence, and young adulthood. They are also unquestionably one of the most powerful vehicles for instrumentarianism in our modern age: as digital signals monitor and track our daily activities, a company may gradually "master the schedule of reinforcements—rewards, recognition, or praise that can reliably produce the specific user behaviors that the company selects for dominance" (Zuboff 2019, 295).

Young people are especially vulnerable to instrumentarian tools on social media. This is because young people are still going through the developmental processes that build individual identity and personal autonomy. In one international study of media use by youth that spanned ten countries and five continents, participants were asked to abstain from all digital media for only twenty-four hours—what emerged was "a planet-wide gnashing of teeth and tearing of flesh that even the study's directors found disquieting" (Zuboff 2019, 445). Specifically, researchers found that participants experienced a range of emotional distress summarized into six categories: addiction, failure to unplug, boredom, confusion, distress, and isolation. Sudden disconnection from social media had produced the kinds of cravings, depression, and anxiety which are characteristic of clinically diagnosed addictions. Scholars such as Zuboff, Vallor, and Véliz argue that addiction is a core design of apps. CEOs have admitted as much. As Suhail Doshi of Mixpanel (an analytics firm that sells tools for measuring user interactions to developers) wrote in a post

titled "Mixpanel: How Addictive is Your App?": "Social apps have a stable, consistent and thoroughly addicted user base, with 50 percent of people engaging with social networks for more than five hours a day, and even a small percentage logging time during every waking hour," (Doshi 2014, para. 3). Again, this is especially troubling for young people, who are still developing their capacities for self-control.[24] Furthermore, social media relies heavily on constant comparisons, with users often judging themselves against idealized versions of the lives and bodies of others. This leads people to know themselves from 'the outside looking in'—to understand themselves in virtue of how others see them. The more the need for the 'others' is fed, the less one is able to negotiate the work of self-construction—this failure to attain positive equilibrium between inner and outer life is so devastating that psychologists Daniel Lapsley and Ryan Woodbury argue it is 'at the heart' of most adult personality disorders (Woodbury et al 2016, 152). This cycle of comparison and obsessing over perfection is part of the magnetic pull that social media exerts on young people, which drives them toward more automatic and less voluntary behavior, and "for too many, that behavior shades into the territory of genuine compulsion" (Zuboff 2019, 449). In particular, Zuboff credits Facebook for excelling in this strategy, writing:

> Facebook is the crucible of this new dark science. It aims to perfect the relentless stimulation of social comparison in which natural empathy is manipulated and instrumentalized to modify behavior toward others' ends. This synthetic hive is a devilish pact for a young person. In terms of sheer everyday effectiveness—contact,

[24] The addictive power smartphones hold over us is a subject depicted by many artists and storytellers—as one song goes: "I try to pull the curtains back / Turn you off, but can't detach / When all I want and all I know / Is time spent looking at my phone" (Goldwasser and VanWyngarden, 2018, track 5). It is also interesting to note that the creator of popular sci-fi horror Netflix series *Black Mirror* named his show after what screens look like when they're turned off (Rowney 2018, para. 6).

> logistics, transactions, communications—turn away, and you are lost. And if you simply crave the fusion juice that is proof of life at a certain age and stage—turn away, and you are extinguished (p. 468).

Only time will tell the full effects of generations growing up in such digital environments[25]—but for now, there appears to be real and tangible harms to our mental health when we engage with modern technological goods and services such as social media.

All these are serious harms worthy of more attention than they are given. Yet we endure these and much more when we use modern technological goods and services to access our modern personhood. For when we click agree, we're entering an exploitative system best described as surveillance capitalism, and are harmed by doing so. These harms directly inhibit our ability to enjoy modern lives—whether if it's being flagged by a racist algorithm or being denied a job because your credit score is too low. And especially during our hyper-connected modernity, where our personal data is being used to try to influence us on every screen we look at, never before have we needed to rely on our autonomy to defend against being manipulated for others' ends.

INSTRUMENTARIANISM & IT'S TOOLS

To enjoy our modern personhood, we are increasingly required to use modern technological goods and services. When we do so, corporations sell access to our autonomy to advertisers and other interested third parties. They do this through a new form of power Zuboff calls instrumentarianism—the power to *know* and *shape* human behavior toward other's ends.

[25] Zuboff repeatedly refers to growing up in such environments as growing up in a 'machine hive'—the term 'hive' here draws echoes to Reiman's 'fishbowl' informational panopticon. Indeed, playing with this these terms further, one might come to understand social media as a sort of pleasurable prison for young people—a hive, sweet and alluring, but inevitably unfulfilling. After all, only one bee has true autonomy: the queen, who orchestrates the rest of her subjects.

Although the phrase "instrumentarianism" is referencing the instrumentation and instrumentalization of behavior for the purposes of modification, prediction, monetization, and control, Zuboff also thought of this phrase in the form of puppetry, writing: "In this formulation, 'instrumentation' refers to the puppet: the ubiquitous connected material architecture of sensate computation that renders, interprets, and actuates human experience" (Zuboff 2019, 376). In our modern technological infrastructure, the *knowing* component to this power refers to how corporations surveil us, while the *shaping* component to this power refers to how corporations use tools of instrumentarianism if exert undue influence over us. Converging technological innovations have dramatically increased what all can be *known* from the information extracted through surveillance, while developments in behavior modification technologies have dramatically increased the effectiveness of behaviors being *shaped*. The existing tools of instrumentarianism appear to be successful enough to at the very least be problematic, and without any regulation on these tools or the power behind them we have good reason to worry about how these tools will develop in the near future.

The tools of instrumentarianism exist through the ubiquitous digital apparatus supporting our modern technological goods and services. Through this apparatus, instrumentarian tools render, monitor, compute, and modify our behavior. Current tools of instrumentarianism include tuning, herding, and conditioning. Tuning is when micro-interventions occur to one's choice architecture: the ways in which situations are already structured to channel attention and shape behavior. A classic example are social media feeds, where corporations decide what posts are prioritized, which photos are highlighted and which news articles you'll encounter while scrolling. Also called nudging, tuning often operates outside of our awareness. Herding involves controlling key elements in a person's immediate context. Under surveillance capitalism, this could look like

a car manufacturer shutting down a driver's car remotely because the driver's late on their car insurance payments. This foreclose of action alternative moves behavior along heightened probability akin to certainty: the driver must drive, after all. Conditioning is the process through which specific behavior is shaped with the application of negative and positive reinforcements. As previously mentioned, smartphones appear to be the primary vehicle for this sort of instrumentarian tool. All three of these tools existed before surveillance capitalism, but what makes these tools so powerful now is the degree to which they're able to *know* our behavior due to our diminished privacy through surveillance technologies, and the degree to which they're able to *shape* our behavior due to both how saturated our digital economy is with these tools and our dependency on modern technological goods and services which force us to interact with these tools on a daily basis. As one of the senior software engineers Zuboff interviewed describes it: "It's no longer about ubiquitous computing, now the real aim is ubiquitous intervention, action, and control … the real power is that now you can modify real-time actions in the real world … real-time analytics translate into real-time action" (Zuboff 2019, 292).

How effective are our current tools of instrumentarianism? Enough to warrant serious concern. Thus far, they've been effective enough to convince advertisers to spend millions upon millions of dollars for them. So effective, in fact, that these revenues made corporations like Google and Facebook some of the most powerful corporations in the world. Digital nudging for the sake of commercial interests appears to be effective at complicating at least some amount of customer autonomy: as one chief data scientist for a drugstore chain put it: "You can make people do things with this technology … even if it's just 5% of people, you've made 5% percent of people do an action they otherwise wouldn't have done, so to some extent there is an element of the user's loss of self-control" (Zuboff 2019, 294). And in 2012, Facebook released results from an

experiment their users to see how effective tuning could be at increasing voter turnout. They concluded that social messaging was indeed an effective means of tuning behavior at scale because "it directly influenced political self-expression, information seeking, and real-world voting behavior of millions of people"—specifically, they calculated that their manipulated social messages sent 60,000 additional voters to the polls in the 2010 midterm election, as well as another 280,000 who cast votes as a result of the "social contagion" effect produced by the tools of instrumentarianism (Zuboff 2019, 299). In the wake of these results, Jonathan Zittrain acknowledged that it's now possible to imagine Facebook quietly engineering[26] an election, using means that its users could neither detect nor control (Zuboff 2019, 300). The "social contagion" effect from this study echoes another experiment Facebook conducted on its users. By manipulating the extent to which people were exposed to certain emotional expressions in their news feed, researchers concluded that emotional states can be transferred to others via emotional contagion, leading people to experience the same emotions without their awareness (Zuboff 2019, 302). It is worth noting that these sorts of experiments are a huge problem: because it is a corporation, Facebook avoids legal standards that academic or governmental researchers are held too. This is what allowed Facebook to experiment on the psychologies of approximately 61 million people without their consent. Add to this that what's being experimented on is voter turnout and user emotions, and these experiments appear profoundly unethical. Part of what allows Facebook such effective emotional manipulation is how much they know about us: an internal document acquired by the Australian press in May 2017 revealed that Facebook was able to target the precise

[26] It is worth noting that corporations are not the only actors manufacturing reality through modern technological goods and services. There have been multiple instances of fake accounts organizing real-world events such as protests and counter protests. In May of 2017, Facebook had to remove roughly 30 real-world events that were organized in this way (Frenkel 2018, para. 7).

moment when users felt nervous, stressed, defeated, silly, or useless—a good thing for Facebook to know, as it is in these moments that we're much more vulnerable to Facebook's tools of instrumentarianism (Zuboff 2019, 304).

A key element to Facebook and other corporations' implementation of instrumentarian tools like tuning, herding, and conditioning is the fact that so much of this process takes place without our awareness. This is because awareness is linked to our autonomy; there is no autonomous judgement without awareness because awareness is a necessary condition for the motivation of cognitive and existential resources, according to theorists Dylan Wagner and Tod Heatherton. They argue that the primary purpose of self-awareness is to enable self-regulation (Zuboff 2019, 307). Regulating our thoughts, emotions, and desires is key to human autonomy. Others, such as researchers at Cambridge University, argue that the single most important determinant of one's ability to resist persuasion is the ability to premeditate, to self-regulate and chart one's own course (Zuboff 2019, 307). This ability conflicts with the goals of surveillance capitalism and its tools of instrumentarianism. Simply put, the more autonomous we are the more we are able to resist the practices which make surveillance capitalists' corporations so rich.

It remains to be seen how instrumentarian tools will develop in the future. Currently, little to no regulation exists to curtail how these technologies are developed or deployed. Corporations have proven quite effective at lobbying against such legislation, just as they have proven quite effective at labeling how exactly these technologies work and all that they're able to know and shape as patentable trade secrets. If surveillance capitalism is logically compelled to diminish our privacy as much as possible so as to effectively deploy, develop, and perfect tools of instrumentarianism—and there appears to be no meaningful way to hinder them—then we have no reason to think the progression of these tools will stop. And because we as customers are less

valuable than others' predictions about our future behavior, corporations are financially compelled to pursue these tools in order to produce predictions as accurate as possible—thereby making them financially compelled to control us as much as possible to realize their own predictions. Baked into the logic of surveillance capitalists is their alleged right to modify others' behavior for profit according to methods that bypass human awareness, individual decision rights, and the entire complex of self-regulatory processes that we can otherwise understand as our autonomy, our experiencing ourselves as the source of the things we do. So far, this declaration has gone unchallenged. Rosalind Picard says the goal of emotion analytics is to render both conscious and unconscious emotion as observable behavior for coding and calculation (Zuboff 2019, 285). Considering how facial recognition software is now capable of detecting one's sexuality, this goal seems plausible.

All of this seems to suggest an extremely worrying future, especially in regard to how surveillance capitalism has restructured our society (i.e. division of learning, the disruption of traditional consumer-product dynamics). Political theorist Hannah Arendt predicted this future decades ago when we began conceiving of our thoughts and our brain as electronic instruments. According to Arendt, the problem with the theories of behaviorism which support these tools isn't that they're wrong, but they could become true, that they are actually the best possible way of conceptualizing of certain obvious trends in modern society. She argues that it's "quite conceivable that the modern age—which began with such an unprecedented and promising outburst of human activity—may end in the deadliest, most sterile passivity history has ever known" (Zuboff 2019, 382). Simply put, the worry here is that the tools of instrumentarianism could lead to the automation of the self as a necessary condition of the automation of society—all for the sake of others' profits. The worry here is that these tools will continue to cut away at our mental wilds to

the point where our autonomy cannot be sustained—at the very least, in the meaningful sort way which allows the sort of autonomy we would classify as human.

THE INTOLERABLE THREAT OF INSTRUMENTARIANISM

The degree to which surveillance capitalism diminishes our privacy is alone problematic for our autonomy. The harms this system produces—from damaging the mental health of younger generations to privatizing the division of learning in our society, from perpetuating discrimination and inequality to bolstering corporate power over democratic governments—are unacceptable. Now with the tools of instrumentarianism, corporations sell access to our autonomy. These tools currently complicate our autonomy in problematic ways, but the potential threat that future instrumentarian tools pose to our autonomy is too dangerous to ignore. To have our autonomy disrupted and made vulnerable in such a way is to endure an intolerable harm.

Recall earlier commentary on how instrumentarian tools can make roughly 5% of people do an action they otherwise wouldn't have done. Perhaps it is the case that we might be okay with these tools making people buy things they wouldn't have otherwise bought. This is essentially the goal of advertising, after all. Yet would we be okay with 5% percent of people voting for a candidate they otherwise wouldn't have voted for if these tools weren't implemented? 5% is more than enough to sway elections. Would we feel better about these tools if only 1% of people had their beliefs manipulated, were made to believe something false about the world that influenced they way they feel and live? What if instrumentarian tools were successfully deployed to make only a handful of people fall into suicidal depression or only a handful of people violently hateful towards a certain race? I don't think we'd be okay with this. We accept that ads might alter our behavior—*to a point*. The difference between instrumentarian tools and traditional advertising is

that instrumentarianism is not mere persuasion. These tools are powered by a profound seizure of our privacy, and they access our autonomy in a way traditional advertising does not. Recall earlier commentary on how recent technological innovations grant instrumentarian tools the power to know others more than they know themselves. The worry here is that instrumentarian tools push something like targeted advertising into targeted manipulation: by leveraging intimate details about ourselves we might not even know, instrumentarian tools allow others to exert this influence in getting us to act, think, or desire in ways we otherwise wouldn't have. Furthermore, instrumentarian tools operate without our awareness, while advertisements are legally required to label themselves as ads. Advertisers would very much like not to label their ads as ads, because when we know an ad is an ad it is less effective at persuading us. We've long acknowledged it is in the public interest to regulate advertising—we've yet to do the same for the surveillance technologies and tools of instrumentarianism which govern our modern technological goods and services. And even if it was the case that these tools were just the future of advertising, the nature of how they operate (that they our powered by our severely diminished privacy, that they directly seek to disrupt our autonomy) makes them morally unacceptable under eudaimonic and technomoral virtues ethics.

Both eudaimonic and technomoral virtue ethics stress the role our autonomy plays in our ability to act and live well. After all, an important part of any virtue ethics is our ability to cultivate virtues: this process cannot be automatic, but a form of conscious deliberation through which we meaningfully choose the good life. By diminishing our privacy, surveillance technologies cut away this space for free moral and cultural play, where we come to hone our virtues because we correctly choose to, not because we're coerced to. As Vallor herself asks: "If surveillance and nudging technologies are marketed and embraced as yet one more social license to relinquish [the struggle

for humans to exercise their moral agency], so that our moral lives may quietly and seamlessly mold into the shapes programmed by Silicon Valley software engineers and technocrats … will we become more or less like the human beings we wish to be?" (Vallor 2016, 204). Furthermore, instrumentarianism completely disregards the role for human autonomy—something that is even more offensive under eudaimonic ethics, as our autonomy is one of our deepest psychological needs. Additionally, it's worth mentioning that surveillance capitalism and its tools of instrumentarianism are also completely unacceptable under Kantian morality, as they make customers and users no longer ends in themselves but rather as means to others' ends. In this new economic order, autonomous thought and moral judgement are unpredictable influences that compete with the influences that instrumentarianism seeks to impose, and therefore must be extinguished.

Because our modern technological goods and services are governed by this logic, using them appears to complicate the cultivation of nearly all technomoral and eudaimonic virtues. As previously stated, cultivating the eudaimonic virtue of autonomy conflicts with instrumentarian tools. But relatedness is also threatened—after all, one of the more surprising effects of social media has been how it increases rates of depression and loneliness (Primack et al 2017, para. 5). Competence can also be understood as under threat given the privatization of the division of learning in society. The sheer amount of knowledge locked away from us—both the knowledge about ourselves as well as the knowledge of how these technologies operate—hinders our ability to hone our skills in a way that makes contributions to our physical and social environment. Meanwhile, the technomoral virtue of self-control is threatened by how advanced techniques in software design magnify the addictive qualities of apps. The technomoral virtue of honesty is complicated by information and communication technologies that continue to aid and abet the

distortion of truth, and the technomoral virtue of justice is complicated by the fact that modern technological goods and services perpetuate discrimination and inequality. More arguments can be made for each virtue, but I believe for now it is clear that the instrumentarian tools saturating our modern technological goods and services hinder our capacity to live virtuously under technomoral and eudaimonic virtue ethics.

Still, this is not to say that our modern technological goods and services themselves are incompatible with living and acting virtuously. There is nothing about these goods and services which requires our diminished privacy and threatened autonomy. We need not sacrifice our right to privacy just to access our other rights. Our technology doesn't have to be designed to expose our autonomy. For Vallor, behavior modification technologies are outright unacceptable because automating our moral agency is unacceptable. But Besser-Jones counters that automatic behavior is not mindless behavior simply because it occurs outside of our conscious awareness, because it does not entail that the behavior does not still reflect an agent's beliefs about how and why they ought to treat others well. In other words, automaticity can be a force of good, and we must only better understand it so we may use it to our advantage (in this case, in our pursuit of acting well, in pursuit of the good life). I find both views compelling: there does seem to be something profoundly dissatisfying about automating away our moral agency even if doing so helps us cultivate our virtues, but there does seem to be room for at least some of these technologies to be permissible so long as we are the ones controlling them. For example, such tools would no longer exert the power of instrumentarianism, because instead of *someone else* knowing and shaping our behavior toward *their ends*, these tools would instead allow *us* to know and shape our own behavior for *our own ends*. I don't believe we need to resolve this tension between these two ethics systems, however; even though they disagree on the potential for these tools to act in service of cultivating

our virtues, they both vehemently agree that these tools in their current use are immoral and incompatible with our virtues.

Furthermore, even if these tools in their current form weren't problematic enough to conflict with eudaimonic and technomoral virtue ethics, we have good reason to fear what future versions of these tools might imply. If instrumentarian tools are perfected and remain unregulated, then our autonomy does indeed appear to be in great danger. This is the conclusion of Zuboff, who warns that "just as industrial civilization flourished at the expense of nature and now threatens to cost us the Earth, an information civilization shaped by surveillance capitalism and its new instrumentarian power will thrive at the expense of human nature and will threaten to cost us our humanity" (Zuboff 2019, 12). Here, humanity refers not only to our autonomy engendered through our privacy, but the values and morals we as a species uphold for ourselves. Historian Yuval Noah Harari also imagines what our increasingly tech-dependent future has in store, specifically for the growing disparity between those wealthy enough to benefit from emerging behavior-modifying technologies and those poor and completely unprepared for such invasions and manipulative methods. In fact, many scholars warn of the growing gap between the wealthy and the poor, of how the rich continue to have access to beneficial technologies long before they trickle down to the middle and lower classes. This is typically understood as how the quality of life rises: what was a luxury for one generation becomes an expected good for the next. In modern times, we're witnessing a slight inversion of this trend, with "the privileged" being serviced more by people, "the masses by machines" (O'Neil 2016, 8). This is what leads him to claim that the most important fact about living in the 21st century is that we are now hackable animals. "To hack a human being," says Harari, "is to understand what's happening inside you on the level of the body, of the brain,

of the mind, so that you can predict what people will do … the real key is whether somebody can understand you better than you understand yourself" (Thompson 2018, para. 15).

This is an interesting thought experiment, one of many which could be made when imagining all the ways instrumentarian tools could develop in the future. The potential threat these tools pose to our autonomy should give us great pause in evaluating the morality of our technosocial contract, which appears to offer us our modern personhood in exchange for the potential dismantling of our modern personhood through the elimination of our autonomy. Specifically, this elimination could be realized if instrumentarianism diminishes our autonomy below the threshold that's required for an act, thought, or desire to be considered autonomous. As previously argued, we might not care as much when we lose autonomy while shopping at a store, but we do care if we lose autonomy when it comes to intimate matters of the self. If our autonomy is cancelled regarding acts, thoughts, and desires through which we form our identity, political and religious convictions, or decisions on important life choices, then we fail to experience our authentic selves as the source of the things we do and instrumentarianism proves to be an intolerable threat.

Part IV: Consent & Coercion

CURRENT THEORIES ON CONSENT & COERCION

To assess whether or not our technosocial contract is justified given the context of surveillance capitalism and its tools of instrumentarianism, I will be looking to leading theories on consent and coercion. Consent is important because if enjoying the goods of modern life entails threats to our privacy, those threats become permissible so long as people consent to diminishing their privacy in order to access these goods. It is through consent that this exchange succeeds or fails to be morally transformative.

One of the most influential contemporary scholars on consent is Alan Wertheimer. He argues that consent is best understood as a bilateral transaction between the consenter and the recipient of consent. Consent and consent transactions place importance on the well-being or interests of the agent, as well as the agent's autonomy. In collaboration with Franklin G. Miller, they argue for what they call a fair transaction model for consent transactions:

> A is morally permitted to proceed on the basis of a consent transaction if A has treated B fairly and responds in a reasonable manner to B's token or expression of consent or what A reasonably believes is B's token or expression of consent. (p. 81)

Moral transformation refers to the process through which an action becomes morally permissible, whereas without this process it would be morally impermissible to follow through. For consent to be morally transformative, both sides of the transaction must be treated fairly, under the correct conditions. This is what leads them to argue that in most contexts "no means no" whereas there are many contexts where we shouldn't assume "yes means yes"—this is the difference between morally transformative consent and valid consent. They conclude that although morally

transformative consent generally tracks valid consent, this is not always the case, and therefore the presence of valid consent alone is not sufficient for moral transformation. In doing so, they don't mean to suggest other conceptions of consent such as informed consent aren't useful, but that they believe the "deeper ethical truth is that it is moral transformation that matters" (Wertheimer and Miller 2010, 101). Consider two partners about to engage in sexual intercourse where one partner is blackout drunk. The intoxicated partner provides valid consent by vocalizing and affirming their consent to sex, but complications arise as most would agree this consent is not morally transformative: most would agree that this it is not a case of meaningful consent. Wertheimer and Miller argue that the correct conditions for fair treatment on consent transactions are when consent is voluntary, informed, and competent. Whether these conditions are met or not is extremely context dependent; it's impossible for an individual to fulfill these conditions perfectly.

Informed consent is an important branch of consent scholarship. It has been influential in bioethics, but other fields are ripe for its application. As noted previously, the overwhelming majority of individuals do not fully read terms and conditions before agreeing to whatever privacy policy their given technological good or service is requiring them to agree to. Furthermore, even if individuals read through these terms and conditions, it is unclear if they can be truly said to be informed, as most still do not know the depths to which their privacy is diminished, nor how these terms and conditions exploit and harm them and their loved ones—and they certainly aren't aware of the instrumentarian tools deployed against them after clicking agree. This has led many to consider informed consent an important concept to consider when crafting privacy policies.

According to philosophers Tom Beauchamp and Ruth R. Faden, autonomy is important for informed consent. They argue it is in virtue of autonomous authorization that we feel satisfied in an act being one of informed consent. Autonomous authorization occurs when 1) one assumes

responsibility for what one has authorized and transfers to someone else the authority to implement it, and 2) one also understands these features of the act and intends to perform that act (Beauchamp et al 1986, 280). They frame autonomous actions as: "X acts autonomously only if X acts 1) intentionally, 2) with understanding and 3) without controlling influences" (Beauchamp et al 1986, 238). They further qualify that informed consent is an ideal, and that though it's rare for people's actions to ever be fully autonomous, we can still promote a certain threshold of autonomy we want to uphold in our conception of consent. And in order for people to reach this standard, there is a certain level of intentionality, understanding, and privacy (what Beauchamp and Faden refer to as our actions occurring without controlling influences) that must be met.

Coercion is important because as long as scholars across disciplines have defined and revised the concept of coercion, the consensus has been that coercion invalidates consent, that coercion cannot coexist with consent. This is because coercion complicates our autonomy by effectively forcing us to do something we would rather not do but do so anyways because we feel we have no other choice—perhaps because we're threatened or saw no other legitimate alternative. An interesting feature of coercion is the facade of legitimacy: after someone has 'forced' someone else to do something they didn't want to do, the person coerced is thought to have consented—at least, until this 'forcing' is properly recognized. Coercion does not always work like this, but it is worth noting how often coercion does work like this.

Traditional philosophical views hold that threats coerce but offers do not—a stance Wertheimer agrees with, as its consistent with his two-prong theory of coercion. Modeling his theory after an expansive review of US law, he argues that a contract is made under duress only if 1) the consenter has no choice and 2) the propositions in the contract are morally wrong

(Wertheimer 1987, 40). According to Wertheimer, the distinction which allows threats to coerce but not offers can be summarized as through the following:

> A *threatens* B by proposing to make B *worse* off relative to some baseline. More precisely, A makes a threat when, If B does NOT accept A's proposal, B will be worse off than in the relevant baseline position. A makes an offer when, if B dot NOT accept A's proposal, he will be no worse off than in the relevant baseline position (p. 204).

Beauchamp and Faden agree with Wertheimer that threats coerce whereas offers do not. They argue coercion only occurs if 1) the agent of influence intends to influence the other person by presenting a severe threat and 2) if this threat is credible and irresistible (Beauchamp and Faden 1986, 261).

Other scholars have put forth alternative models of coercion which seem applicable in examining our technosocial contract—specifically, that offers can indeed be coercive. David Zimmerman argues that "the intuitive idea underlying coercion is that the person who does the coercing undermines or limits the freedom of the person who is coerced" (Zimmerman 1981, 134). Using a model of coercion set by Michael Garnett, he argues that an offer is coercive only if an individual would prefer to move from the normally expected pre-proposal situation to the proposal situation, but he would strongly prefer even more to move from the actual pre-proposal situation to some alternative pre-proposal situation. Zimmerman uses the example of capitalist wages offers to show how offers may prove coercive. Many scholars have debated whether or not the wage bargain in a capitalist labor market is coercive if the worker is limited to a choice between unpalatable alternatives, such as choosing to either work at a low-paying, miserable job or go starving. According to Zimmerman, a wage offer is coercive if and only if 1) an alternative pre-proposal situation workers would strongly prefer to the actual one is technologically and

economically feasible when the offer is made, and 2) capitalists prevent workers from having at least one of these feasible alternative pre-proposal situations (Zimmerman 1981, 145). Joan McGregor offers another way of understanding coercive offers after examing the marketplace in terms of bargaining power. According to McGregor, offers may coerce when the effect on the individual asking to consent is a choice between evils, the lesser of which is to acquiesce—in other words, threats put the victim in a vulnerable position, but offers find the victim in a vulnerable position, where "the weaker party has no workable alternatives since there is collusion in the industry making actual alternatives an illusion" (McGregor 1988, 45).

Again, the dominant view in current philosophy on consent and coercion is that threats coerce but offers do not. Beauchamp and Faden argue that coercive offers aren't coercive because even if an offer is made in a setting in which it is abnormally attractive, it would be better classified as manipulation or some other sort of wrong. Much of their hesitancy to allow exploitation to qualify as coercion seems to come back to concerns over who caused the miserable state of affairs for the consenter. Other times, they argue that "freedom-enhancing exploitative offers do not coerce" because they expand rather than reduce one's options relative to one's moral baselines (Wertheimer 1987, 233).

APPLYING THE CONTEXT OF OUR TECHNOSCIAL CONTRACT

Although these philosophers disagree on whether or not an offer may be coercive, all agree that whether or not consent has been coerced depends on the specific context of the contract in question. When we consider the context of our technosocial contract—all the harms surveillance capitalism entails, the instrumentarian tools which cut away our mental wilds to access our autonomy—then there does indeed appear to be something problematic about exchanging privacy

for access to modern technological goods and services. If an individual declines to consent, they are denied the means to realize modern personhood and fulfill their autonomy—an unbearable harm. But if an individual accepts, then they're entering an exploitative system of various harms where instrumentarian tools endanger their autonomy. A case could be made that both options are psychologically unrealistic to expect people to choose. But considering how immediate the threat of denied modern personhood is, compared to how delayed the harms from surveillance capitalism might be and how instrumentarian tools often exert undue influence over us without our awareness, then it seems that psychological realism would hold that it is illogical to expect people to choose the immediate and more obvious harm of denied modern personhood. Still, choosing between an unbearable harm and an intolerable harm doesn't seem like much of a choice; this exchange doesn't feel morally transformative.

Although Wertheimer, Miller, Beauchamp, and Faden would say that an offer cannot coerce (and our technosocial contract does indeed appear to be some sort of offer) their theories on consent suggest that there is something about our technosocial contract which fails to yield morally transformative consent. Regarding Wertheimer and Miller's Fair Transaction Model, it seems dubious at best to claim that corporations are treating us fairly. After all, corporations control modern technological goods and services—essentially monopolizing access to the goods of life and our fulfillment of modern personhood. Note here how much control they have over these, too: they choose which content we can access, they control what platforms we use to connect with others, shop, and work. We have no alternatives. Then they outright claim our human experience as free raw material for them to profit off of. They deploy instrumentarian tools (which we often don't even know about) to access our autonomy, exerting undue influence over us in order to alter our behaviors, desires, and emotions in service of their commercial interests. Nothing

about this is fair. Furthermore, surveillance capitalist corporations have a habit of not responding in a reasonable manner to our token of consent—specifically when we decline to give our consent. There have been many cases where corporations find ways to surveil us even if we click disagree—a prominent example of this is Facebook, which is able to surveil all web users (including non-Facebook users) through the "Like" button being embedded on sites across the internet (Zuboff 2019, 158). Even if users disable the browser plug-in Google Toolbar, studies have shown that Google continues to surveil them through this plug-in across competing search engines (Zuboff 2019, 131). Meanwhile, when we click disagree we often run the risk of corporations punishing us for doing so[27]: as one illuminating example, Nest is a smart thermostat made by Google. Should a customer refuse to agree to Nest's terms of agreement (consisting of nearly a thousand so-called contracts), the device will not work properly, with consequences ranging from frozen pipes to failed smoke alarms to an easily hackable internal home system (Zuboff 2019, 7). All of this seems to suggest that our technosocial contract should not be considered a fair transaction. Perhaps it yields valid consent by technicality, but it is not morally transformative—which is the sort of consent Wertheimer is concerned with.

Another way our technosocial contract fails at being morally transformative for Wertheimer is through the nature of wrongful proposals. According to Wertheimer, it is wrong to propose to do that which is independently illegal, while it is generally not wrong to propose to exercise a legal right (Wertheimer 1987, 38). According to eudaimonic and technomoral virtues ethics, our technosocial contract is making a proposal that is morally wrong because it directly

[27] As seen with Nest, this typically involves corporations rendering devices inoperable—not because devices like vacuums or fridges desperately need to diminish our privacy and render our autonomy exploitable in order to function, but because surveillance capitalist corporations make more money when they do so.

conflicts with the cultivation of the virtues we care about. While it is the case that most of what our technosocial contract is imposing is technically legal, it is not clear that what's being imposed stems from corporations' legal rights. It's important to recall that when surveillance capitalism originated with Google, they were breaching into territory that was unregulated and incomprehensible to even those in the tech industry at the time. In fact, investors were initially impressed and mystified at how Google earned so much profits without selling any material assets. Furthermore, regulation on surveillance technologies as well as legislation protecting consumer privacy has been outpaced by the developing technologies within surveillance capitalism, and there's currently no regulation on tools of instrumentarianism. Throughout American history, powerful corporations have used the Constitution to fight off unwanted government regulations.[28] As previously mentioned, Zuboff credits the success of surveillance capitalism to the neoliberal policies that surged in the wake of 9/11. Neoliberalism can be generally understood as the political theory that personal liberty is maximized when government interference in the free market is limited. Often associated with laissez-faire economics, neoliberal policies seek to limit government regulation over corporations as much as possible. According to Zuboff, these policies initiated a "slow and transformative shift tying our social needs inextricably with corporations" (Zuboff 2019, 40). As it stands, however, corporations do not have an explicit legal right to be surveilling us or using instrumentarianism against us. Moreover, we as citizens in a democracy define the rights

[28] Although corporations have also used the Constitution to fight off unconstitutional regulations, here I refer to corporate America's history of using the Constitution to fight off regulations they merely don't want but would otherwise be constitutional and beneficial for consumers. One way we see this under surveillance capitalism is through free speech fundamentalism. This concept holds that individuals have an absolute right to free speech. According to Zuboff, surveillance capitalists have deflected scrutiny over their operations by shielding themselves behind the First Amendment—all while their practices are antidemocratic in spirit and in effect hinder an individual's ability to speak freely (Zuboff 2019, 110).

corporations are entitled to—not the other way around. What I argue is that our technosocial contract functions as a wrongful proposal under Wertheimer's framework. Just because this proposal isn't illegal doesn't mean it's not wrongful. We have good reason to regard this proposal as morally wrongful, just as we also have good reason to regulate or in some cases outright ban some of the practices that is inside this proposal. Wertheimer himself admits that there are exceptions to his conception of wrongful proposals—I believe we have good reason to consider the context of our technosocial contract as one of them.

It's also worth noting that an important component to Wertheimer's understanding of coercion is how duress can make a proposal qualify as coercive. While the second prong of his theory deals with the wrongfulness of a proposal, the first prong deals with whether an individual had any reasonable or acceptable alternative. In other words, a contract might prove coercive if an individual is under duress and feels they have no choice—Wertheimer believes that some version of this theory provides the best account of coercion in his review of contract law (Wertheimer 1987, 36). As previously outlined throughout this project, the conditions surveillance capitalism imposes upon us could certainly constitute duress. If so, then even if an individual had nothing to do with bringing about this duress, any token of consent exchanged could still fail to be morally transformative.

Likewise, Beauchamp and Faden's conception of informed consent appears wildly incompatible with our technosocial contract. First and foremost, surveillance capitalism's privatization of the division of learning—and the profound asymmetry in knowledge it produces—should make us wary of the average individual's ability to understand what exactly is being asked of them in our technosocial contract. And as I've previously explained, converging technological innovations have allowed us to extract more information than ever before. While it could be said

an individual acts intentionally, we have good reason to doubt an individual in this scenario could act with understanding—and they're certainly not acting without controlling influences. After all, consenting to this technosocial contract means signing up to be bombarded by instrumentarian tools seeking to control us by exerting undue influence us. Additionally, Beauchamp and Faden base their understanding of autonomy specifically through Kant, and they believe their framework for informed consent is consistent with the Kantian conception of autonomy. As I've argued earlier, our technosocial contract goes against Kant's conception of autonomy to the point that we would be morally required to click disagree. This (as well as previous points) seems to suggest that our technosocial contract is not conducive to autonomous authorization, and therefore not conducive to informed consent.

Given the context of our technosocial contract, it appears that Wertheimer, Miller, Beauchamp, and Faden would indeed find something problematic about this exchange—yet they withhold the term coercion, and argue that offers cannot coerce. But they also do not identify what exactly is wrong about this exchange, just that seems to fail at being morally transformative. Until they address what that problem is, I believe we can move on and consider how our technosocial contract could classify as coercion.

THE LOGIC OF COERCIVE OFFERS

Before I address how our technosocial contract does indeed appear to act as a coercive offer, I want to revisit Wertheimer's critique of coercive offers as well as what appears to be the most common rebuttal against the existence of coercive offers: that exploitative offers do not coerce so long as they're mutually beneficial or freedom-enhancing.

According to Wertheimer, threats coerce because they propose to make someone worse off than they would otherwise be, whereas offers do not coerce because if someone declines this proposal than they're no worse off than they were before. Yet it does not logically follow that offers cannot coerce. Let's say I'm on a sinking ship and I do not know how to swim. A lifeboat passes by offering to ferry me to shore, but only in exchange for me and any of my potential heirs to be in service to them forever. If I decline, I'll drown, so of course I "consent" to this exchange. This would be a coercive offer.[29] Wertheimer would agree with this. In other words, this offer functions as both offer and threat—the offer is safe passage home, and the threat is that if I decline this offer then I will drown. In applying this to our technosocial contract, the offer is access to modern technological goods and services at the cost of our privacy and therefore autonomy, and the threat is being denied our modern personhood. We can extrapolate more threats from this exchange—as NSA whistleblower Edward Snowden comments in his memoir aptly titled *Permanent Record*, the unilateral collection of everyone's data carried the tantamount threat that if you ever got out of line, your private life could be used against you. "Imagine it," he writes, "all the secrets big and small that could end your marriage, end your career, poison even your closest relationships, and then leave you broke, friendless, and in prison," (Snowden 2019, 198). Such secrets—from the sequencing of your DNA to swapped nudes with your lover—are now stored by

[29] This example and critique of Wertheimer's argument is similar to that of McGregor, who argues that offers may coerce when the effect on the individual asking to consent is a choice between two evils, the lesser of which is to acquiesce. In other words, threats put the victim in a vulnerable position, but offers find the victim in a vulnerable position, where "the weaker party has no workable alternatives since there is collusion in the industry making actual alternatives an illusion" (McGregor 1988, 45). Under surveillance capitalism, there is certainly collusion among corporations to pressure politicians to keep allowing the dominance of surveillance technologies and instrumentarian tools across our modern technological goods and services.

corporations, governments, and whoever else came across your personal data at is sold, analyzed, and instrumentalized to modify your behavior.

Reconsider how Wertheimer, Miller, Beauchamp, and Faden are hesitant to allow exploitation like this to qualify as coercion due to concerns over who caused the miserable state of affairs for the consenter. After all, the lifeboat passing by me did not cause my ship to sink, and their offer certainly grants me more freedom than a watery death. Aside from the fact that, again, this offer appears to also be a threat, we should question this notion that mutually beneficial exploitative offers or freedom-enhancing exploitative offers do not coerce. Consider the fight for labor rights in the US: for almost half of this nation's history, child labor appeared to be mutually beneficial and therefore not coercive—yet now we would judge this as abhorrent, coercive, and indefensible. In fact, it could be argued that exploitation is always coercive, so long as it's judged in the right context. Now we appreciate the context of child labor which makes it coercive—perhaps in the future we will also appreciate the context which lets us see capitalist wage offers (the main focus of most scholarship for and against coercive offers) as coercive.

What seems to allow exploitative wage offers to be permissible is this notion that employers aren't at fault because they're not the ones who made the employee's conditions so dire. Would we say the same of the employers who used exploitative wage offers to hire children to go work in mines? I don't believe we would. This is because, as Wertheimer notes, we care more about consent being morally transformative than being valid. Exploitative offers might be valid, but they often fail to feel morally transformative—and I argue they feel so because what we care about is that someone is being coerced. Someone or something does indeed have to be coercing in order for someone to be coerced—but they don't necessarily have to be the employer or the person initiating this contract. Again, the lifeboat didn't sink my ship, but I'm nonetheless being coerced.

And at the very least, I argue that we should resist any calls to allow exploitative offers a free pass just because the exchange appears to be mutually beneficial to us right now.

There are two ways we can understand our technosocial contract as a coercive offer—first, through the inherent coercive nature within this exchange, and secondly, through Zimmerman's examination of capitalist wage offers. There are many coercive elements at play within our technosocial contract, but perhaps the most extraordinary coercive element is the fact that this exchange is asking us to consent to endanger our autonomy. Consider the fact that the whole point of this contract is to excuse the invasion of our privacy by having an individual consent. This seems to imply that this exchange cares a great deal about consent. Yet as previously argued, consent hinges on autonomy—we cannot truly be said to consent if we're not doing so autonomously, or at least to a substantial degree. But if we do consent in this exchange, then we are rendering our autonomy exploitable in profound and potentially devastating ways. We might wonder why then we're being asked to autonomously consent in the first place if this exchange is going to then immediately encourage the targeting of our autonomy—that alone seems to suggest something isn't quite right with this offer.

When we push this further, however, a clear coercive element comes into play. By clicking agree, we are entering a marketplace for others to disrupt our autotomy with instrumentarian tools—and if these tools are successful enough, do indeed diminish our autonomy enough, then this thereby damages our ability to autonomously consent on the next inevitable round of this technosocial contract. In other words, by clicking agree we're agreeing to be subjected to tools of instrumentarianism that directly inhibit our ability to click disagree. If the intuitive idea underlying coercion is that my freedom is being undermined by the person or entity coercing me, then our

technosocial contract seems not only coercive, but hypocritical: it claims to care so much about the thing it seeks to immediately snuff out.

The other way we can understand our technosocial contract as a coercive offer is through Zimmerman's examination of capitalist wage offers. First, it should be acknowledged that typical philosophical framing around coercive offers is of wages: an exchange between an employer and employee. I believe Zimmerman convincingly argues that certain capitalist wage offers might be coercive, but what's perhaps even more important is what happens when we apply his strategy to surveillance capitalist offers. Recall how under surveillance capitalism we are neither workers nor consumers, but terrain to harvest from. This is a transformative shift. Before, monopolies on goods and services disfigured markets by unfairly eliminating competition in order to raise prices at will. Under surveillance capitalism, however, many of the practices defined as monopolistic actually function as means of cornering user-derived raw-material supplies, as Zuboff writes: "There is no monetary price for the user to pay, only an opportunity for the company to extract data…. We are the source of the coveted commodity: our experience is the target of extraction," (Zuboff 2019, 132).

I argue there is something inherently coercive in the offer of modern personhood at the cost of what is essentially an economic mutation of indentured servitude: instead of contracting yourself to work for someone else until a certain amount of time has passed, you're contracting yourself to be harvested for raw material and to be subject to instrumentarian tools of behavior modification just so you may access things like social media, healthcare, and education—and for however as long as you wish to enjoy your modern personhood, you will need to continue being monitored, mined, and unduly influenced.

Though a wage offer is of a different sort of offer, Zimmerman's model for coercive offers is still informative. Surveillance capitalist offers certainly seem to fit the spirit of his criteria. It is certainly technologically and economically feasible for us to use modern technological goods and services which don't invade our privacy and threaten our autonomy. I believe it is uncontroversial to claim that this is certainly the preferred alternative pre-proposal situation for most modern citizens. And if capitalists could ever have been said to prevent workers from having at least one feasible alternative pre-proposal situation (i.e. access to non-hazardous, not-horribly paying jobs), then surely it can be reasonably claimed that surveillance capitalists actively seek and are extraordinarily successful at preventing modern citizens from accessing technological goods and services which don't exploit and harm them. This is what Zuboff claims through her conception of the new sort of contractual forms emerging in the wake of surveillance capitalism:

> The uncontract is a feature of the larger complex that is the means of behavioral modification, and it is therefore an essential modality of surveillance capitalism … it contributes to economies of action by leveraging proprietary behavioral surplus to preempt and foreclose action alternatives, thus replacing the indeterminacy of social processes with the determinism of programmed machine processes … The uncontract is not a space of contractual relations but rather a unilateral execution that makes those relations unnecessary (p. 220).

If surveillance capitalists continue to exert effective influence over an individual's ability to access technological goods and services which don't surveil or deploy instrumentarian tools against them, then it seems as though surveillance capitalism easily fulfills the spirit of Zimmerman's criteria: offers are coercive when an alternative pre-proposal situation is feasible and sufficiently better

than the actual offer which capitalists prevent citizens from having alternative options to (Zimmerman 1981, 140).

All of this seems to suggest that we should consider our technosocial contract to be coercive. Although this exchange doesn't fit the narrow definition of coercion of Wertheimer, Miller, Beauchamp, and Faden, I argue that this is the most appropriate term. Specifically, I believe my previous arguments as well as Zimmerman's examination into exploitative capitalist wages suggest that we have good reason to consider this exchange a coercive offer. Recalling Solove's application of Wittgenstein's family of resemblances to the definition of privacy, we might also want to consider coercion as a cluster-concept—at the very least, we shouldn't be afraid to revise our definition of coercion as new contexts require us to. And while it might be the case that Wertheimer Wertheimer, Miller, Beauchamp, and Faden could argue that this exchange is problematic in ways befitting other terminology, this would become a debate over semantics, not whether or not our technosocial contract is capable of producing meaningful consent.

Part V: Conclusion

CLOSING ARGUMENTS

Before I conclude, I will preemptively consider expected arguments against different claims within my overarching thesis. I will begin by examining the GDPR—the toughest privacy security law in the world. The GDPR is the most robust and lauded iteration of our technosocial contract; if I am to argue our current technosocial contract is logically unjustified, then I must also prove the GDPR is equally flawed. The GDPR is aimed at protecting the privacy of citizens in the European Union against data collection and processing. This law does more to address the problems inherent within our technosocial contract than any other laws. Concepts such as the Right to be Forgotten are insightful and indicative of the sort of theorizing we will need to be doing more of in the future.[30] I argue, however, that this law still fails to justify the exchange of privacy for accessing modern technological services. All five "strict new rules" defining what constitutes consent do not address the coercive nature of this exchange, which makes it such that actual consent cannot be given from the very "data subjects" this law aims to protect. Additionally, I echo concerns of scholars such as Véliz, in that this legislation does not go nearly as far enough in protecting our privacy in the age of surveillance capitalism. She argues that certain rules in the

[30] The right to be forgotten is the right to have private information about a person be removed from internet searches and other directories under certain circumstances. Véliz notes that this concept protects us from being haunted by personal data that is outdated, inaccurate, inadequate, irrelevant, or devoid of purpose, and when there is no public interest (Véliz 2020, 149). Given my conception of the goods of modern personhood, it can be reasonably argued that just as there might be a right to be forgotten online, there should be a right to exist online. With social media becoming even more entrenched in the careers, communities, and interactions which seem to characterize our modern life, the fact that corporations retain the sole power over these platforms is frightening. Perhaps the internet would better be reconceptualized as a public utility and social media as a public platform, wherein proper regulation and protections would be subject to civilian oversight.

GDPR are too broad, such as allowing companies to collect data for 'legitimate interests', and that the GDPR still fails to address the issue of anonymized data that can later be deanonymized (Véliz 2020, 131). Surveillance capitalists will often claim that because data is anonymized, there is no way to track the data back to its user, and therefore there are no privacy issues to be had. But because anonymized data can be later de-anonymized, privacy issues can still emerge. It can also be argued that just because data is completely anonymized this doesn't mean our privacy wasn't violated. Some personal data—such as a final phone call to a loved one on their death bed—seems like the sort of personal data in which it would be immoral to automatically seize such private affairs as raw material for others' profit and aims, even if this data were fully anonymized.

A common critique against any attempts to challenge the technological infostructures shredding our privacy and enabling instrumentarianism can be classified as technofatalism: the belief that technological advancement is inevitable, and that emerging surveillance technologies are a part of this inevitability. Technofatalists believe it is naïve and illogical to fight for regulatory or cultural restraints on surveillance technologies, and that there's no effective steering away from this course (Véliz 2020, 193). There seems to be a consensus among current philosophical literature on privacy and technology that technofatalists are incorrect. It's no coincidence that the most rabid technofatalists are surveillance capitalists—Zuboff argues that big tech hopes we will grow gradually accustomed to accepting conditions we would never have agreed to had they been presented to us upfront from the start. Again, the unique circumstances surrounding our technosocial contract seems to suggest coercion. Furthermore, Zuboff clarifies that surveillance capitalism is not technology: it is a logic that imbues technology and commands it into action. Technofatalism is a simply a classic misdirection to bewilder the public by conflating commercial imperatives and technological necessity. I agree with Zuboff and many other scholars such as

Vallor and Véliz that technofatalism is incorrect. Technofatalist critiques of my project can largely be addressed by the previous arguments, but a technofatalist could also claim that it is unrealistic for me to expect the goods of modern life to be so easily accessible without some sort of sacrifice on my part. Yet this too seems surmountable: once again, there is nothing about our modern technological goods and services which requires the economic logic of surveillance capitalism to be structuring this transaction. As Zuboff also argues, surveillance capitalism was invented by a specific group of human beings in a specific time and place—it's not an inherent result of digital technology, nor is it a necessary expression of information capitalism (Zuboff 2019, 85).

It could also be argued that the benefits of surveillance capitalism outweigh the drawbacks. While surveillance technologies and instrumentarian tools have proven to exploit and harm thus far, with proper regulation and civil protections, they could prove to be overwhelming forces of good. A classic proponent of this sort of thinking is behaviorist B. F. Skinner, who believed tools of behavior modification such as conditioning could be used for the greater good. I partially agree with this, as do Vallor and Zuboff: it certainly could be that case that, in certain contexts, surveillance technologies and instrumentarian tools do indeed function as an overwhelming good. Yet we might wonder how the greater good can be determined when surveillance capitalism owns the machines and the means of behavioral modification. As Zuboff writes: "The greater good is someone's good, but it may not be ours," (Zuboff 2019, 432). This is because surveillance capitalism is fundamentally profit driven, specifically driven to extract as much behavioral surplus data as possible while modifying our behavior as discreetly as possible. These conditions do not seem the sort of conditions where the type of well-meaning, overwhelmingly beneficial uses of surveillance technologies and instrumentarian tools can flourish. For example, a traditional technofatalist and pro-surveillance belief is that the more informed a population is, the better off

they will be. Technology ethicists such as Evan Selinger and Woodrow Hartzog argue, however, that there are many empirical studies which show that people suffering a supply of too much information become more passive, less responsible, overwhelmed, and more likely to fall back on dangerous cognitive biases and shortcuts in ethical judgment (Vallor 2016, 193).

Still, other proponents point to Quantified Self practices as potential ways instrumentarianism ultimely servers the great good. These practices entail using wearable devices to collect personal data about one's own life and health. But the problem is that, right now, the tools of instrumentarianism are not being used to make us better, they're being used to sway our political opinions or sell us products. Most nudging, tuning, and conditioning in surveillance capitalism is not designed around self-betterment but around increasing profits. Vallor makes a compelling case against these practices, citing evidence which shows that they do not fulfill the aims of an examined life needed to cultivate virtue and promote sustained human flourishing (much less their own alleged aims), adding that "the most accurate and comprehensive recording of your past and present states would not constitute an examined life, because a dataset is not a life at all" (Vallor 2016, 202).

Secondly, as things currently stand, surveillance capitalists not only monopolize the power of instrumentarianism and enforce a severe power asymmetry of knowledge, but they also monopolize our access to the goods of modern life. The fact that we cannot do things like learn at school or communicate with a loved one far away without contracting ourselves as terrains to harvested from by one of a handful of all-powerful, all-knowing corporations is a testament to how much control surveillance capitalist exert over our capacity to enjoy modern personhood. Surveillance capitalists are unregulated, highly active in lobbying politicians to prevent regulation and funding academic research to manufacture their legitimacy. They can de-platform presidents

and bully countries. Even if surveillance capitalism may sometimes function as an overwhelming force of good, it remains to be seen is it can truly surmount the global sociopolitical threat that corporations wielding instrumentarianism currently pose.

CONCLUSION

The problem with exchanging privacy for accessing modern technological goods and services is that this exchange is incapable of producing meaningful consent. This is because our technosocial contract can be best understood as a coercive offer, and consent cannot coexist with coercion. Even if we do not want to use the term coercion to describe this exchange, leading theories on consent still view this exchange as failing to be morally transformative—meaning this exchange is still incapable of producing meaningful consent. Our technosocial contract therefore remains unjustified. This is a problem, as courts continue to permit this technosocial contract as legally binding, despite being incapable of producing meaningful consent. One solution could be significant legislation severely restricting or banning practices such as the trade in personal data and the use of instrumentarian tools. Other solutions could include curtailing the use surveillance technologies and behavior modification technologies, and ending practices of default data collection across corporations, institutions, and governments. At the very least, we need further scholarship advising our politicians and judicial officials that there should be a new and justifiable technosocial contract.

The loss of our mental wilds just entails too many harms to ignore. Perpetuating discrimination and inequality, bolstering corporate control over both the goods of modern life and democratic governments, hoarding the tools we need to live virtuously and flourish as human beings—surveillance capitalism and its tools of instrumentarianism now seek to consume our

mental wilds, byte by byte, with the potential of one day swallowing our autonomy whole. And of all the fallouts from this siege, among the many tragedies is the loss of these mental wilds for the young to grow up in. There are no artificial wilds, after all. Just as future generations might not enjoy environmental conditions like an unpolluted shoreline or rain that's not acidic, so are they also positioned to not experience the environmental conditions favorable to privacy and the production of their autonomy as generations before them enjoyed. Adding to this tragedy is how the privatization of the division of knowledge lets surveillance capitalist corporations manufacture their reality. What might become of a people made entirely of tuners and their tuned? They divide. One ascends, rendering the other as total means to an end. This other isn't even an 'other': plucked of their human nature, the tuned stops functioning as people at all.

References

Anderson, M. (2015). "6 Facts about Americans and their Smartphones." *Pew Research Center*. https://www.pewresearch.org/fact-tank/2015/04/01/6-facts-about-americans-and-their-smartphones/.

Besser-Jones, L. (2017). *Eudaimonic Ethics*. Routledge.

Bloodworth, A. (2018, April). "Do Grindr and Other Dating Apps Affect Mental Health?" *Pink News*. https://www.pinknews.co.uk/2018/04/18/does-grindr-affect-mental-health-dating-apps-and-mental-health/.

Browne, S. (2015). *Dark Matters: On the Surveillance of Blackness*. Duke University Press.

Crawford, K., Richardson, R., & Schultz, J. (2019). Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. *New York University Law Review, 94*(192). Retrieved 2019, from https://www.ssrn.com.

Doshi, S. (2014). "Mixpanel: How Addictive Is Your App?" *Vox.* https://www.vox.com/2014/3/6/11624264/mixpanel-how-addictive-is-your-app.

Faden, R. R., & Beauchamp, T. L. (Eds.). (1986). *A History and Theory of Informed Consent*. Oxford University Press.

Foucault, M. (1995). *Discipline & Punish: The Birth of the Prison*. Vintage Books.

Frenkel, S. (2018). "How a Fake Group on Facebook Created Real Protests." *New York Times*. https://www.nytimes.com/2018/08/14/technology/facebook-disinformation-black-elevation.html.

GDPR - User-Friendly Guide to General Data Protection Regulation . General Data Protection Regulation. (2018). https://www.gdpreu.org/.

Haro, A. (2017, February 27). “Chilling Prediction From Biologists Warns that 50% of All Species Could be Extinct by End of Century”. *The Inertia*. https://www.theinertia.com/environment/chilling-prediction-from-biologists-warns-that-50-of-all-species-could-be-extinct-by-the-end-of-the-century/.

Kolbert, E. (2014). *The Sixth Extinction*. Henry Holt and Company.

Korsgaard, C. (2009). *Self-Constitution*. Oxford University Press.

Leopold, A. (1949). *A Sand County Almanac: And Sketches Here and There*. Oxford University Press.

Ludwig , W. (1921). *Tractatus Logico-Philosophicus*. Annalen der Naturphilosophie.

McGregor, J. (1988). Bargaining Advantages and Coercion in the Market. *Philosophy Research Archives*.

*“*Mobile Fact Sheet.” *Pew Research Center*. (2021, April 7). https://www.pewresearch.org/internet/fact-sheet/mobile/.

Mokrosinska, D. (2017). Privacy and Autonomy: On Some Misconceptions Concerning the Political Dimensions of Privacy. *Law and Philosophy*, *37*(117). https://doi.org/https://doi.org/10.1007/s10982-017-9307-3

Nissenbaum, H. (2010). *Privacy In Context*. Stanford University Press.

O'Neil, C. (2016). *Weapons of Math Destruction*. Broadway Books.

Pasquale, F. (2016). *The Black Box Society*. Harvard University Press.

Primack, B. A., Shensa, A., Sidani, J. E., Whaite, E. O., Lin, L. Y., Rosen, D., … Miller, E. (2017). Social Media Use and Perceived Social Isolation Among Young Adults in the U.S . *American Jounral of Preventive Medicine*. https://doi.org/10.1016/j.amepre.2017.01.010

Rowney, J.-A. (2018). “Why Black Mirror is called Black Mirror.” *Mirror*. https://www.mirror.co.uk/tv/tv-news/black-mirror-called-black-mirror-11831977.

Sensen, O. (Ed.). (2013). *Kant on Moral Autonomy*. Cambridge University Press.

Snowden, E. (2019). *Permanent Record*. Metropolitan Books.

“Social Media Fact Sheet.” *Pew Research Center*. (2021, April). https://www.pewresearch.org/internet/fact-sheet/social-media/.

Solove, D. (2001). Conceptualizing Privacy. *California Law Review*, *90*(4), 1087–1155. https://www.jstor.org/stable/3481326.

Tankovska, H. (2021, January). “Number of Grindr DAU and MAU worldwide 2018.” *Statista*. https://www.statista.com/statistics/719621/grindr-user-number/.

Thompson, N. (2018). “How Humans Get Hacked: Yuval Noah Harari & Tristan Harris Talk with Wired.” *Wired*. https://www.wired.com/video/watch/yuval-harari-tristan-harris-humans-get-hacked.

Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. *First Monday*, *19*(7). https://doi.org/http://dx.doi.org/10.5210/fm.v19i7.4901

Vallor, S. (2016). *Technology and the Virtues*. Oxford University Press.

Véliz, C. (2020). *Privacy Is Power*. Bantam Press.

Wang, Y., & Kosinski, M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of Personality and Social Psychology*. https://doi.org/https://doi.org/10.1037/pspa0000098

Watson, H. (2018). “How Obsessed Is Gen Z With Mobile Technology?” *The Center for Generational Kinetics.* https://genhq.com/how-obsessed-is-gen-z-with-mobile-technology/.

Watson, J., Venter, O., Lee, J., Jones, K. R., Robinson, J. G., Possingham, H. P., & Allan, J. R. (2018). “Protect the last of the wild." *Nature*. https://doi.org/https://doi.org/10.1038/d41586-018-07183-6

Wertheimer, A. (1987). *Coercion*. Princeton University Press.

Wertheimer, A., & Miller, F. G. (Eds.). (2010). *The Ethics of Consent*. Oxford University Press.

Wood, C. (2018, April). “WhatsApp photo drug dealer caught by 'groundbreaking' work.” *BBC News*. https://www.bbc.com/news/uk-wales-43711477.

Woodbury, R. D., & Lapsley , D. (2016). Social Cognitive Development in Emerging Adulthood. In J. J. Arnett (Ed.), *The Oxford Handbook of Emerging Adulthood* . essay, Oxford Library of Psychology.

Zareen, N., Karim, N., & Khan, U. A. (2016). Psycho Emotional Impact of Social Media Emojis. *ISRA Medical Journal, 8*(4).

Zimmerman, D. (1981). Coercive Wage Offers. *Philosophy & Public Affairs*, *10*(2), 121–145.

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. Profile Books.