



University of Pennsylvania  
**ScholarlyCommons**

---

Honors Theses (PPE)

Philosophy, Politics and Economics


---

5-5-2022

## User-Generated Collateral Data as Property: A Philosophical Argument for Implementing a Property Rights Framework for Data at the Global Human Rights Level

Aakruti Ganeshan  
*University of Pennsylvania*

Follow this and additional works at: [https://repository.upenn.edu/ppe\\_honors](https://repository.upenn.edu/ppe_honors)

 Part of the [Comparative Politics Commons](#), [Defense and Security Studies Commons](#), [Ethics and Political Philosophy Commons](#), [Political Theory Commons](#), and the [Public Policy Commons](#)

---

Ganeshan, Aakruti, "User-Generated Collateral Data as Property: A Philosophical Argument for Implementing a Property Rights Framework for Data at the Global Human Rights Level" (2022). *Honors Theses (PPE)*. Paper 48.

This paper is posted at ScholarlyCommons. [https://repository.upenn.edu/ppe\\_honors/48](https://repository.upenn.edu/ppe_honors/48)  
For more information, please contact [repository@pobox.upenn.edu](mailto:repository@pobox.upenn.edu).

---

# User-Generated Collateral Data as Property: A Philosophical Argument for Implementing a Property Rights Framework for Data at the Global Human Rights Level

## Abstract

The advent of the digital age has borne a new economic ideology, termed “surveillance capitalism” by Shoshanna Zuboff, whereby technological corporations extract valuable behavioral insights from swaths of user-generated “collateral” data to amass profit. The employment of surveillance capitalist logic results in several pernicious harms to the individual and the collective. In this thesis, I argue that surveillance capitalism poses specific threats to freedom, autonomy, and distributive justice. Previous scholarship has conceptualized the right to data through the lens of privacy. However, I posit that a framework of property rights may be better suited to address surveillance capitalisms' threats. I reference the landscape of data privacy laws, as well as a broader argument as to the global nature of cyberspace, to establish that privacy laws in isolation cannot remediate the harms resulting from surveillance capitalism. Subsequently, this paper makes two crucial arguments: first, that the injuries wrought by surveillance capitalism necessitate the designation of the “right to data” as a human right. Referencing the works of John Rawls, Charles Beitz, and Joseph Raz, I advance the claim that the right to data is justified by the same normative principles used to justify the existing practice of human rights. The second major premise indicates that property rights will adequately address surveillance capitalism’s threats to autonomy, freedom, and distributive justice. In the following sections of the thesis, I explore possible practical manifestations of the property rights framework and consider relevant objections to the argument.

## Keywords

internet, surveillance capitalism, human rights, property rights, big data, distributive justice, data privacy, facebook, amazon, international

## Disciplines

Comparative Politics | Defense and Security Studies | Ethics and Political Philosophy | Political Theory | Public Policy

**User-Generated Collateral Data as Property: A  
Philosophical Argument for Implementing a Property Rights  
Framework for Data at the Global Human Rights Level**

Aakruti Ganeshan

*Submitted to the Philosophy, Politics and Economics Program at the University of Pennsylvania  
in partial fulfillment of the requirements for Honors.*

Thesis Advisor(s): Carlos Pereira Di Salvo

Date of Submission: May 5, 2022

USER GENERATED COLLATERAL DATA AS PROPERTY: A PHILOSOPHICAL  
ARGUMENT FOR IMPLEMENTING A PROPERTY RIGHTS FRAMEWORK FOR DATA  
AT THE HUMAN RIGHTS LEVEL

COPYRIGHT

2021

Aakruti Ganeshan

This work is licensed under the  
Creative Commons Attribution-  
NonCommercial-ShareAlike 3.0  
License

To view a copy of this license, visit

<https://creativecommons.org/licenses/by-nc-sa/3.0/us/>

## ACKNOWLEDGMENTS

This thesis would not have been possible without the support, guidance, and counsel of numerous individuals over the last few months.

Thank you to my advisor, Dr. Carlos Pereira di Salvo, whose continual feedback over the course of the semester proved invaluable to my final project. You have inspired me to delve into philosophical research with an expansive mindset, and to challenge myself in both conducting research and making logical arguments. I would not have been able to embark upon such an ambitious and technical project without your expertise.

Thank you to the Philosophy, Politics and Economics (PPE) Department at the University of Pennsylvania for providing me with the opportunity to write this thesis, and for stimulating my interest in an interdisciplinary topic. I would also like to thank Dr. Eileen Doherty-Sil for provoking my interest in the field of human rights and encouraging me to pursue it in my thesis.

I would also like to express my gratitude to my friends at Penn and abroad. Your words of kindness and support have been invaluable in motivating me to complete this project. I would especially like to thank Tirtha Kharel for providing me with insights into the world of computer science and data analytics that informed my base understanding of the subjects broached in this paper.

Lastly, I would like to thank my family for their love and guidance. My mother and father have both made the completion of this project possible through their persistent assurances and words of encouragement.

## ABSTRACT

The advent of the digital age has borne a new economic ideology, termed “surveillance capitalism” by Shoshanna Zuboff, whereby technological corporations extract valuable behavioral insights from large swaths of user-generated data to amass huge amounts of profit. This “collateral” data is generated by the user through daily interactions with the internet and is obtained and processed by corporations either with or without the consent of the user. The employment of surveillance capitalist logic results in several pernicious harms to both the individual and the collective. In this thesis, I argue that surveillance capitalism poses specific threats to freedom, autonomy, and distributive justice. Previous scholarship has conceptualized the right to data through the lens of privacy. However, I posit that a framework of property rights may be better suited to address the threats produced by surveillance capitalism. I reference the landscape of current and future data privacy laws, as well as a broader argument as to the global nature of cyberspace, to establish that privacy laws in isolation cannot remediate the harms resulting from surveillance capitalism. Subsequently, this paper makes two crucial arguments: first, that the injuries wrought by surveillance capitalism are severe enough to necessitate the designation of the “right to data” as a human right. Referencing the works of John Rawls, Charles Beitz, and Joseph Raz, I advance the claim that the right to data is justified by the same normative principles used to justify the existing practice of human rights. The second major premise indicates that property rights will adequately address surveillance capitalism’s threats to autonomy, freedom, and distributive justice. In the following sections of the paper, I explore possible practical manifestations of the property rights framework and consider relevant objections to the argument.

# TABLE OF CONTENTS

<b>ACKNOWLEDGMENTS</b>	3
<b>Introduction</b>	7
<b>Section 1: Historical Origins of the Internet and Data Collection</b>	9
<b>Section 2: Clarifying the Harms Produced by Surveillance Capitalism</b>	14
Section 2A: The Threat to Autonomy	15
Section 2B: The Threat to Freedom	19
Section 2C: The Threat to Distributive Justice	23
Section 2D: On the universality of autonomy, freedom and distributive justice.	26
<b>Section 3: Exploring Current Conceptions of Data Ownership and Privacy</b>	30
Section 3A: Justifying Data Protections at the International Level	30
Section 3B: Surveying the Landscape of Data Privacy	32
<b>Section 4: Justifying The Right to Data as a Human Right</b>	36
Section 4A: Grounding the Political Conception Argument for Human Rights	37
Section 4B: Establishing the Right to Data as a Human Right	42
<b>Section 5: Justifying the Right to Data Under a Property Framework</b>	49
Section 5A: The Pre-Existing Right to Property in the Human Rights Corpus	49
Section 5B: Defining Property	53
Section 5C: Defining Data as Property	54

Section 5D: Examining How the Property Right to Data can Address Surveillance	
Capitalism's Harms	56
<b>Section 6: Objections to the Argument for Data as Property</b>	<b>65</b>
<b>Conclusion</b>	<b>67</b>
<b>Bibliography</b>	<b>69</b>



## Introduction

The notion of a “digital footprint” – digital traces that users leave behind as they surf the internet or go online – has become relatively commonplace in the 21st century. Individuals sign away the records of their online behavior on a daily basis, often by absentmindedly clicking “accept” on an obscure list of terms and conditions or accessing websites that surreptitiously record their behavior.<sup>1</sup> As innocuous as this phenomenon may seem, these human experiences are digitized and translated into behavioral data for use by corporations. In a process that has come to be termed as “surveillance capitalism,” technological firms can wield seemingly insignificant behavioral data to make powerful predictions about human behavior.<sup>2</sup>

The logic of surveillance capitalism is often construed as a mechanism employed by internet companies to fine-tune online advertising, largely in the name of accurately targeting personalized advertisements to consumers. However, in recent years, this phenomenon has accelerated far beyond the realm of targeted advertising. The 2018 Cambridge Analytica case demonstrates that surveillance capitalism can actually *shift* human behavior to affect political outcomes and obstruct the democratic process.<sup>3</sup> This is just one example of the detrimental harms resulting from surveillance capitalism; recent research has shown that companies can synthesize insights gleaned from user behavior on the internet to determine credit scores and eligibility for premium insurance policies.<sup>4</sup> These instances illustrate some of the negative

---

<sup>1</sup> “DIGITAL FOOTPRINT (Noun).” In *Macmillan Dictionary*. Accessed December 8, 2021. <https://www.macmillandictionary.com/us/dictionary/american/digital-footprint>.

<sup>2</sup> Shoshanna Zuboff. *The Age of Surveillance Capitalism*. (New York City: PublicAffairs Books, 2018), 18

<sup>3</sup> Alex Hern, “Cambridge Analytica: How Did It Turn Clicks into Votes?” *The Guardian*, May 6, 2018, sec. News, <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>.

<sup>4</sup> Robert H. Sloan and Richard Warner, “Algorithms and Human Freedom,” *Santa Clara High Technology Law Journal* 35, no. 4 (March 13, 2019), <https://doi.org/10.2139/ssrn.3351960>.

impacts of surveillance capitalism. I will delve into a more detailed description of the precise harms in Section 2 of this paper.

Given that this process is relatively new, very little legislation is currently in place to protect individuals from potential harms generated through surveillance capitalist tactics. Consumers virtually have no control over the data they generate, nor do they wield any tactical power over how their data is used. Zuboff describes the mechanisms through which the exact process occurs, claiming that the collateral behavioral data generated by users from interacting with the internet, i.e., “data exhaust,”<sup>5</sup> is converted by companies into specific “prediction products”<sup>6</sup> that are used to predict (and possibly shape) user behavior. There are two key processes at play here: first, that this behavioral data is often collected surreptitiously or without user knowledge. Second, even with the presence of terms and conditions and “opt-out” functions, users frequently relinquish their privacy rights over data without second thought.

While existing approaches to the regulation of surveillance capitalism typically focus on bolstering user privacy, in this thesis, I will make an argument for a framework of property rights over the raw data exhaust that users generate. Importantly, I do not intend to justify user ownership over the prediction products that companies generate from user data. Rather, I intend to establish a right to the collateral data that users generate through interfacing with the internet in myriad ways: whether it be from surfing the web, using social media, or wearing a trackable activity device. More specifically, I intend to claim that this right to data (as I will refer to it) should be institutionalized within the international human rights practice.

After delving into the history of surveillance capitalism in Section 1, I will detail its precise harms to both the self and society, including threats to autonomy, freedom, and

---

<sup>5</sup> Zuboff, *The Age of Surveillance Capitalism*, 110.

<sup>6</sup> Zuboff, *The Age of Surveillance Capitalism*, 18.

distributive justice. I will then specify why the right to data is already encompassed by the existing breadth of human rights regimes. To do so, I will utilize one of the two philosophical lenses that are commonly associated with the justification for human rights: the “political conception,” which argues that the nature of human rights is best understood by their current, distinct role in international political practice. Lastly, I will examine why a framework of “data as property” may serve as appropriate redress for the harms produced by surveillance capitalism and explore practical manifestations of this framework.

### **Section 1: Historical Origins of the Internet and Data Collection**

Leonard Kleinrock published the first paper on “packet switching theory,” a globally interconnected set of computers that transferred data in packets for efficiency.<sup>7</sup> Concurrently, the first large scale packet-switching network, ARPANET, was built by the Advanced Research Projects Agency (ARPA) in 1969.<sup>8</sup> A product of the U.S Department of Defense’s research initiatives, the ARPANET computer network linked more than 50 government agencies and universities all over the United States.<sup>9</sup> This instigated the creation of several other packet-switching networks, like the packet radio system PRNET and the satellite communications network SATNET.<sup>10</sup>

To effectively connect different heterogeneous networks, Vinton Cerf and Robert Kahn designed the TCP/IP, or the “Internet Protocol,” which was formally adopted by every host site on each network by 1983.<sup>11</sup> Throughout the mid-80s and the 90s, the National Science

---

<sup>7</sup> Barry M Leiner, Robert E Kahn, and Jon Postel. “A Brief History of the Internet.” *ACM SIGCOMM Computer Communication Review* 39, no. 5 (October 2009): 23, <https://dl.acm.org/doi/10.1145/1629607.1629613>

<sup>8</sup> See above.

<sup>9</sup> Abbate, Janet. *Inventing the Internet*. Inside Technology.(Cambridge: MIT Press, 1999)

<sup>10</sup> John Naughton, “The Evolution of the Internet: From Military Experiment to General Purpose Technology.” *Journal of Cyber Policy* 1, no. 1 (May 2016): 5–28, <https://doi.org/10.1080/23738871.2016.1157619>.

<sup>11</sup> Abbate, *Inventing the Internet*.

Foundation (NSF) funded a series of supercomputing centers around the United States, forming the NSFNET network that would become the backbone of the “civilian network.”<sup>12</sup> Following the decommission of ARPANET in 1990, the internet was privatized by Internet Service Providers (ISPs), expanding network access to laypeople. Around the same time, the scientist Sir Tim Berners-Lee created the “WorldWideWeb,” the internet’s first web browser and editor, using pre-established hypertext software. This development set the stage for the first “Internet Boom” in the 90s.<sup>13</sup>

In the spring of 1993, Eric Bina and Marc Andreessen released “Mosaic,” the first web browser that displayed graphics inline. Mosaic precipitated a surge in the demand for internet connections among the general public, triggering several other companies to begin offering commercial browsers and search engines.<sup>14</sup> Among these search engines was Google, a startup founded by Larry Page and Sergey Brins in the wake of Mosaic’s success. As users began engaging with the web through Google’s services, these computer mediated activities produced large swaths of data.

Every Google search query would create an abundance of collateral information, like the “number and pattern of search terms, how a query is phrased, spelling, punctuation, dwell times, click patterns, and location.”<sup>15</sup> Upon realizing that these data could provide valuable insights into user behavior, Google’s engineers grasped that they could use this flow of collateral information to turn the search engine into a “recursive learning system.”<sup>16</sup> Zuboff refers to this as the “behavioral value reinvestment cycle,” a process by which behavioral data from the user was

---

<sup>12</sup> Naughton, “The Evolution of the Internet.”

<sup>13</sup> See above.

<sup>14</sup> Abbate, *Inventing the Internet*.

<sup>15</sup> Zuboff, *The Age of Surveillance Capitalism*, 114.

<sup>16</sup> Zuboff, *The Age of Surveillance Capitalism*, 115.

reinvested in the user's internet experience with the purpose of generating an improved search engine.<sup>17</sup>

Nevertheless, this reinvestment into users was short-lived. When the dot-com bubble crashed in 2000, Google searched for a way to annul the crisis by responding to investors' anxieties. Google tasked its seven member AdWords team with the objective of finding more ways to make money – they quickly learned that they could mine behavioral data to specifically match ads to users' interests. In short, the raw behavioral data that had originally been reinvested in optimizing users' experience was redirected towards predicting user behavior.<sup>18</sup> Key to this was the compilation of data sets called "UPIs" – user profile information – that were created and analyzed from a user's search patterns.<sup>19</sup> This process was so successful in generating revenue that Google eventually extended the model beyond their search pages, rendering the internet a canvas for targeted advertisements.

In academia, scholars identify this extraction of user data in different ways. Viktor Mayer-Schönberger and Kenneth Cukier refer to the initial stages of creating collateral user data as "datafication" – unearthing data from material that was previously considered unimportant.<sup>20</sup> Crucially, datafication is distinct from "digitization," the process of converting analog information into the zeros and ones of binary code for computers, because it involves enlarging the observations captured from an initial data set by expanding the confines of the data set itself. However, the actual logic of *capitalizing* on this dataset to generate profit is better known as

---

<sup>17</sup> Zuboff, *The Age of Surveillance Capitalism*, 117.

<sup>18</sup> Zuboff, *The Age of Surveillance Capitalism*, 115.

<sup>19</sup> Zuboff, *The Age of Surveillance Capitalism*, 132.

<sup>20</sup> Viktor Mayer-Schönberger, and Kenneth Cukier. *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Boston: Houghton Mifflin Harcourt, 2013), 165.

“surveillance capitalism,” a term first coined by Shoshanna Zuboff in 2014.<sup>21</sup> To describe the mechanics of surveillance capitalism, I will appropriate some of Zuboff’s key terms. Data that is originally generated for product or service improvement is declared “proprietary behavioral surplus,” which insinuates that the behavioral surplus is a product owned and trademarked by the respective companies through which the surplus is generated.<sup>22</sup> This behavioral surplus is fed into advanced “machine intelligence” processes, eventually becoming “prediction products that will anticipate what you will do now, soon, and later.”<sup>23</sup>

Google’s employment of surveillance capitalist practices soon provoked a vast array of competitors from every sector: gradually establishing surveillance capitalism as the default model of information capitalism on the web.<sup>24</sup> When Google went public in 2004 and revealed their financial results to the world, Silicon Valley investors became aware of the elusive business model of surveillance capitalism that solidified the company’s success. Four years later, Mark Zuckerberg embarked on a quest to apply Google’s logic and techniques to the Facebook platform by hiring former Google Executive Sheryl Sandberg. Under Sandberg’s direction, Facebook would learn to not only generate behavioral surplus, but also to effectively *create* demand for advertiser’s products by deliberately inviting advertisers into Facebook’s online culture.<sup>25</sup>

In part, surveillance capitalism treats data as a capital asset – a piece of property expected to generate value over time.<sup>26</sup> This conception has proved to be highly profitable to large

---

<sup>21</sup> John Laidler. “Harvard Professor Says Surveillance Capitalism Is Undermining Democracy,” *Harvard Gazette* (blog), March 4, 2019, <https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/>.

<sup>22</sup> Zuboff, *The Age of Surveillance Capitalism*, 20.

<sup>23</sup> Zuboff, *The Age of Surveillance Capitalism*, 19.

<sup>24</sup> Zuboff, *The Age of Surveillance Capitalism*, 155.

<sup>25</sup> Zuboff, *The Age of Surveillance Capitalism*, 154.

<sup>26</sup> “The Rise of Data Capital.” MIT Technology Review Custom, 2016. <https://www.technologyreview.com/2016/03/21/161487/the-rise-of-data-capital/>.

corporations. For example, Amazon’s targeted advertisement system is valued at a staggering \$125 billion.<sup>27</sup> This valuation is because Amazon’s database remediates some of the guesswork present in Google or Facebook’s behavioral database by having direct access to consumer’s delivery addresses, shopping history, and credit card information. Furthermore, in 2016, 89% of the revenues of Google’s parent company “Alphabet” was derived from Google’s targeted advertising programs.<sup>28</sup> Notably, corporations profit off user data without providing any compensation to the users themselves.

A clearer example of Facebook’s behavioral modification was revealed in 2017 through leaked documents obtained by *the Australian*. Essentially, Facebook monitored post, pictures, interactions, and internet activity to pinpoint the precise emotional states of young people at different points in the day. From this information, Facebook could determine when a younger person was most “vulnerable to a specific configuration of subliminal cues and triggers.”<sup>29</sup> This data was then used to match emotional phases with messaging that guaranteed the maximum probability of sales, thus capitalizing on user’s emotions to manipulate their actions.

However, Zuboff argues that this process is problematic on an even more insidious level. Beyond the extraction of behavioral data, surveillance capitalists’ interests have shifted from knowing about behavior to using machine-learning processes to shape it. Since surveillance capitalism is fundamentally an economic process, it can be described in phases of competitive intensity, or the extent to which corporations in the same industry can exert influence over one another and their profits. At the peak of this competitive intensity, extracting behavioral insights

---

<sup>27</sup> Karen Weise, “Amazon Knows What You Buy. And It’s Building a Big Ad Business From It,” *The New York Times*, January 20, 2019, sec. Technology, <https://www.nytimes.com/2019/01/20/technology/amazon-ads-advertising.html>.

<sup>28</sup> Zuboff, *The Age of Surveillance Capitalism*, 149.

<sup>29</sup> Sam Levin, “Facebook Told Advertisers It Can Identify Teens Feeling ‘Insecure’ and ‘Worthless,’” *The Guardian*, May 1, 2017, sec. Technology, <https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens>.

is insufficient in assuring a competitive edge. Instead, surveillance capitalists turn to means of behavioral modification, using machine processes to tacitly shape individual, group, and population behavior.

This phenomenon is perhaps best exemplified by Facebook’s 2012 study, “A 61-million-person experiment in social influence and political mobilization.” Facebook reported that randomly delivered political mobilization messages to Facebook users during the 2010 US congressional election sent an estimated 60,000 additional voters to the polls and delivered 280,000 others who cast votes due to a “social contagion” effect.<sup>30</sup> These results provide insight as to how surveillance capitalists can leverage their influence to modify and change human behavior.

## **Section 2: Clarifying the Harms Produced by Surveillance Capitalism**

What is the exact issue with surveillance capitalism? While the potential ramifications and harms to individuals may seem relatively obvious, scholars disagree in their exact identification of the problem. In the following section, I intend to outline the harms surveillance capitalism poses to individual autonomy, freedom, and distributive justice.

Here, I will note that the logic of surveillance capitalism yields products like personalized content and an individualized user experience, which may be considered beneficial to users. Furthermore, some users actively *desire* this individualized experience; a survey conducted by Epsilon and GBH Insights of 1,000 American respondents found that 80% want personalization from retailers.<sup>31</sup> It could also be argued that corporations’ profits from surveillance capitalism

---

<sup>30</sup> Robert M. Bond et al., “A 61-Million-Person Experiment in Social Influence and Political Mobilization,” *Nature* 489, no. 7415 (September 2012): 295–98, <https://doi.org/10.1038/nature11421>.

<sup>31</sup> Erik Lindecrantz, Madeleine Tjon Pian Gi, and Stefano Zerbi, “Personalized Experience for Customers: Driving Differentiation in Retail | McKinsey,” *McKinsey & Company*, April 28, 2020,



have yielded indirect economic benefits. For instance, Google’s search and advertising tools have helped provide \$426 billions in productive economic activity.<sup>32</sup> However, these profits are achieved at the cost of several important harms that cannot be dismissed.

In Section 5D of this paper, I will detail a possible implementation of my proposed framework that will allow for targeted, personalized content (and associated profits), without resulting in the same negative repercussions to autonomy, freedom, and justice. Given that there is a way to achieve an individualized user experience and productive economic activity without incurring the negative ramifications, I contend that the positive outcomes of surveillance capitalism do not eliminate the need for potential remedies. Even if a detractor of this argument were to disagree my proposed solution, I will make the case that the harms posed by surveillance capitalism necessitate *some* sort of solution that still allows for the constructive benefits to flourish. To this end, I will proceed with an analysis of the possible threats of this practice.

### *Section 2A: The Threat to Autonomy*

Richard Herschel and Virginia M. Miori highlight a variety of broad ethical implications to do with “Big Data,” a nebulous phenomenon that they define as the process of “capturing, storing, sharing, evaluating and acting upon information that humans and devices create and distribute using computer-based technologies and networks.”<sup>33</sup> Big Data, in conjunction with algorithms and machine learning, forms the crux of surveillance capitalism. It is important to note that it is not Big Data itself that is problematic, rather, it is the way in which Big Data is

---

<https://www.mckinsey.com/industries/retail/our-insights/personalizing-the-customer-experience-driving-differentiation-in-retail>.

<sup>32</sup> “Google Economic Impact,” Google, accessed November 12, 2020, <https://economicimpact.google.com/introduction/>.

<sup>33</sup> Richard Herschel and Virginia M. Miori, “Ethics & Big Data,” *Technology in Society*, no. 49 (May 2017): 31–36, <https://doi.org/10.1038/nature11421>.<sup>6/5/2022 3:50:00 PM</sup>

employed that generates harm. Since a number of academic scholars have written about the ethical nature of Big Data, I will refer to their analysis insofar as it applies to the specific practice of surveillance capitalism, while using the term Big Data when discussing their original articles.

Herschel and Miori discuss Big Data in the context of four broad ethical perspectives. First, they claim that Big Data fundamentally challenges the ethical standard represented by the Kantian viewpoint: namely, that one should always respect the autonomy of other people, treating them as ends in themselves as opposed to treating individuals as mere means to an end.<sup>34</sup> Under Kant's definition, the "autonomy of the will" is "the property of the will by which it is a law to itself independent of any property of the objects of volition." In layman terms, a person is "autonomous only if his choices and actions are unaffected by factors that are external, or inessential to himself," where the "external factors" are heavily contingent on situation and context.<sup>35</sup>

Under this definition, I argue that since surveillance capitalism heavily relies on the surreptitious collection and analysis of data without user consent, an individual's ability to make choices that are "unaffected by inessential factors" is challenged. Surveillance capitalism's tactics of distilling individuals down to data points, marketing to assumed preferences, and shaping consumer behavior constitute "external or internal factors" that interfere with free will by attempting to predict and modify human behavior. For an example of specific behavioral modification, see the preceding section discussing Facebook's targeting of specific mood points to shape consumer preferences, which demonstrates how surveillance capitalism constitutes an external factor that influences consumer preferences.

---

<sup>34</sup> Herschel and Miori, "Ethics & Big Data."

<sup>35</sup> Taylor, J. Stacey, "Autonomy." *Encyclopedia Britannica*, June 20, 2017. <https://www.britannica.com/topic/autonomy>.

Even in cases where individuals are given the chance to “opt-out” of surveillance capitalist tactics, people often fall victim to “euphemisms of consent,” a term I will discuss in greater detail at a later point in this paper. Briefly, the personal autonomy offered by terms and conditions contracts and opt-in/opt-out options is a guise, because individuals often sign their rights away without further thought. Also, because there is no practical mechanism through which users can monitor where their information is going, individuals are often unaware of the extent to which their data is being shared. This is a clear violation of the autonomy prioritized by Kantian ethics, because surveillance capitalism assumes a user’s consent to data collection and impinges on their free will through behavioral manipulation.

A similar conclusion can be reached without relying on a distinctively Kantian conception of autonomy. Sofia Grafanaki adopts the broader view that autonomy concerns not just a person’s actions, but also the independence and authenticity of the desires (like values and emotions) that instigate them to act in the first place.<sup>36</sup> Autonomy, then, is conceived of in two stages: an exploration phase where an individual develops the capacity and ability for choice (i.e.: individual self-determination), and a second stage where an individual applies their own original thoughts and conceptions to a specific act or decision. On this view, surveillance capitalism undermines autonomy by threatening the exploration phase.<sup>37</sup>

The extraction of behavioral data and creation of user profiles often determines what choices an individual will be given online. These choices can be relatively trivial, such as a user receiving ads for only certain types of products, but they can also be more harmful, like selective marketing for housing, insurance, credit decisions or career opportunities. This selective

---

<sup>36</sup> Sofia Grafanaki, “Autonomy Challenges in the Age of Big Data,” *Fordham Intellectual Property, Media and Entertainment Law Journal* 27, no. 4 (May 2017): 810, <https://ir.lawnet.fordham.edu/iplj/vol27/iss4/3>

<sup>37</sup> See above.

marketing discriminates between users based on the behavioral data collected from them. In this sense, the machine learning processes employed by surveillance capitalism can create “self-fulfilling prophecies,” wherein the data being used to make predictions about an individual are themselves being used to shape their behavior. As such, since predictions are not independent of an individual’s eventual decisions, such machine learning processes diminish an individual’s capacity for choice.

Interestingly, Grafanaki also highlights what she terms “Orwellian concerns,” with regards to the effects of surveillance capitalism on the second stage of autonomy.<sup>38</sup> A Pew Research report found that writers, globally, are overwhelmingly worried about mass surveillance and engaging in self-censorship. Another report found that the Edward Snowden revelations have amplified concerns about data surveillance, thus limiting expression and exploration at the personal level online.<sup>39</sup> This argument echoes Foucault’s metaphor of the “panopticon,” where the threat of continuous surveillance drives people to modulate their behavior.<sup>40</sup> Though these concerns are largely to do with governmental, rather than corporate, surveillance, the key principle can be extrapolated to surveillance capitalism. The unmonitored surveillance of online behavior interferes with an individual’s ability for self-determination and expression on the internet.<sup>41</sup>

---

<sup>38</sup> Grafanaki, “Autonomy Challenges,” 817.

<sup>39</sup> “Global Chilling: The Impact of Mass Surveillance on International Writers.” PEN American Center, January 5, 2015, <https://pen.org/research-resources/global-chilling/>.

<sup>40</sup> Michel Foucault, “‘Panopticism’ from ‘Discipline & Punish: The Birth of the Prison,’” *Race/Ethnicity: Multidisciplinary Global Contexts* 2, no. 1 (2008): 1–12, <http://www.jstor.org/stable/25594995>

<sup>41</sup> There is disagreement as to this specific claim, as some research claims that individuals now resign themselves to hyper-visibility rather than actively engaging in self-censorship. See Grafanaki’s article for more information.

*Section 2B: The Threat to Freedom*

Surveillance capitalism also provokes concerns regarding freedom, more often referred to as liberty. Liberty is a multifaceted concept. The most famous distinction between types of liberty is Isaiah Berlin's concept of positive and negative liberty. Positive liberty is labeled as "self-mastery," or the ability to be in control of one's life in being self-directed and autonomous.<sup>42</sup> Negative liberty refers to a "freedom from interference, coercion, or restraint" from other people and entities.<sup>43</sup>

There is much academic debate about the applicability of these two concepts. Some scholars, such as Gerald MacCallum, have even suggested that the dichotomy between positive and negative liberty is a false one and that there are instead a range of possible interpretations of "freedom."<sup>44</sup> For the purposes of my argument, I will utilize Amartya Sen's definition of freedom, which involves not just the absence of certain social forces, but also the presence of certain capabilities. This view does not necessarily fall under Berlin's original conception of positive liberty, despite bearing some similarity to the self mastery argument. I have chosen to use this particular conception of freedom because it holds a certain degree of multicultural value in being applicable to a wide range of cultures, an argument which I will explain in Section 2D.

Capabilities, according to Sen, are defined as the "real freedoms that people have to achieve their potential doings and beings."<sup>45</sup> In this sense, real freedom constitutes having the

---

<sup>42</sup> Ian Carter, "Positive and Negative Liberty," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, (Metaphysics Research Lab, Stanford University, 2021), <https://plato.stanford.edu/archives/win2021/entries/liberty-positive-negative/>.

<sup>43</sup> Steven Heyman, "Positive and Negative Liberty," *Chicago-Kent Law Review* 68, no. 1 (December 1992): 81, <https://scholarship.kentlaw.iit.edu/cklawreview/vol68/iss1/10>

<sup>44</sup> Carter, "Positive and Negative Liberty."

<sup>45</sup> Ingrid Robeyns and Morten Fibieger Byskov, "The Capability Approach," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Winter 2021 (Metaphysics Research Lab, Stanford University, 2021), <https://plato.stanford.edu/archives/win2021/entries/capability-approach/>.

means necessary to achieving potential doings or beings rather than exclusively focusing on the formal freedom to do or be something. Sen's analysis concludes that the appropriate space to assess human equality and advantage is through the capabilities they have "reason to value."<sup>46</sup> However, his original formulation of the capabilities approach does not specify *which* capabilities people should have reason to value. His view does not tell us which freedoms are relevant and should be considered fundamental as opposed to other wants and needs. Martha Nussbaum's extension of Sen's argument assumes a set of universal values, allowing her to specify a list of ten central capabilities that may not be compromised.

Given the range of epistemological concerns that arise because of committing to any central list of human capabilities, I will avoid resorting to Nussbaum's universal list of capabilities, and instead adhere to Sen's original argument.<sup>47</sup> Sen distinguishes between the capability to achieve functioning relevant to one's being ("the well-being aspect") and the capability to pursue goals other than the pursuit of one's well-being ("the agency aspect").<sup>48</sup> The well-being aspect involves a vector of functionings that are constitutive of a person's being, including elementary functions such as being well-nourished and avoiding escapable mortality as well as more complex pursuits like community involvement and self-respect.<sup>49</sup> The capability to achieve such functions essential to well-being is what constitutes substantive freedom.

Concomitantly, an individual's capability to gain achievements that they value (but that may not

---

<sup>46</sup> Nuno Martins, "Realism, Universalism and Capabilities," *Review of Social Economy* 65, no. 3 (2007): 253–78, <https://www.jstor.org/stable/29770415>

<sup>47</sup> David Clark, "The Capability Approach: Its Development, Critiques and Recent Advances," *Global Poverty Research Group 2* (January 2005), [https://base.socioeco.org/docs/developments\\_critiques\\_advances.pdf](https://base.socioeco.org/docs/developments_critiques_advances.pdf)

<sup>48</sup> Amartya Sen, "Functionings and Capability," in *Inequality Reexamined* (Oxford: Oxford University Press, 1995), <https://doi.org/10.1093/0198289286.003.0004>.

<sup>49</sup> See above.

necessarily contribute to their well-being in the way the well-being aspect involves) constitutes their agency freedom.<sup>50</sup>

I will now turn to an examination of how surveillance capitalism interferes with an individual's capability to achieve their well-being. I posit that surveillance capitalism interferes with capabilities through the synthesis of "broad-based predictions."<sup>51</sup> Robert Sloan and Richard Warner use this term to describe how insights obtained from virtually any area of one's online presence, through algorithms and machine learning processes, can inform vital components of their future. These insights can contribute to a person's insurance policies, employment opportunities, and even credit scores. This is a phenomenon I will detail further in the succeeding section on distributive justice. Nevertheless, with regards to credit scores, Rob Aitken describes how "alternative data" that includes social networking patterns can contribute to the formalization of credit scores for those without credit records or files (a group of people he calls the "unbanked").<sup>52</sup>

To situate this example within the context of surveillance capitalism, the data exhaust generated from social networking activity (in conjunction with other alternative data) is put through algorithmic processes that yield predictive products which determine an individual's credit score. Given that credit scores are hugely significant in determining financial status, this example illustrates how surveillance capitalism can interfere with an individual's capability to take out loans, have insurance, and obtain employment. In modern society, these functions are

---

<sup>50</sup> Amartya Sen, "Freedom, Agency and Well-Being," in *Inequality Reexamined* (Oxford: Oxford University Press, 1995), <https://doi.org/10.1093/0198289286.003.0005>.

<sup>51</sup> Sloan and Warner, "Algorithms and Human Freedom."

<sup>52</sup> Rob Aitken, "'All Data Is Credit Data': Constituting the Unbanked." *Competition & Change* 21 (June 20, 2017): 281, <https://doi.org/10.1177/1024529417712830>.

inevitably associated with well-being; therefore, this example illustrates how surveillance capitalism may interfere with an individual's capability to achieve well-being.

Another instance of surveillance capitalism infringing on capabilities occurs in the context of freedom of speech, spirit, and opinion. The capability for speech, spirit and opinion may not be integral to well-being, but it is a function that many have reason to value. Thus, we might consider it to be encompassed by Sen's agency aspect. While there are variances in global attitudes, a Pew Research Center survey found that a majority of people in 38 countries polled (including the U.S, Latin America, Europe, Asia, the Middle East and Africa) consider the freedom of expression to be important.<sup>53</sup>

The synthesis of prediction products leads to consumer personalization, which exposes users to the same sorts of views, beliefs, and decisions that have been gleaned from their original user profile. According to Henrik Sætra, this propagation of mimetic ideas leads to a "narrowing" of the world we perceive, creating "algorithm-based filter bubbles."<sup>54</sup> Surveillance capitalism limits the capability for freedom of expression and opinion by perpetuating "bubbles" with like-minded spirit and opinions through algorithmic filters. This argument is echoed by Janneke Gerard, who claims that the internet and online presences are indispensable to the freedom of expression and the access to information.<sup>55</sup> In narrowing the wealth of information available to users based on predictive products about their tastes, the logic of surveillance capitalism limits the capability for individuals to partake in freedom of expression.

---

<sup>53</sup> Richard Wike and Katie Simmons, "Global Support for Principle of Free Expression, but Opposition to Some Forms of Speech" (Pew Research Center, November 18, 2015), <https://www.pewresearch.org/global/2015/11/18/global-support-for-principle-of-free-expression-but-opposition-to-some-forms-of-speech/>.

<sup>54</sup> Henrik Skaug Sætra, "The Tyranny of Perceived Opinion: Freedom and Information in the Era of Big Data," *Technology in Society* 59 (November 2019): 3, <https://doi.org/10.1016/j.techsoc.2019.101155>.

<sup>55</sup> Janneke Gerards, "The Fundamental Rights Challenges of Algorithms," *Netherlands Quarterly of Human Rights* 37, no. 3 (September 2019): 205–9. <https://doi.org/10.1177/0924051919861773>.



Sætra also argues that the compilation of UPIs designed to make us purchase specific products and services, click on news stories, vote, and pay taxes comprises “nudges” that interfere with the agency aspect. This manipulation threatens the capability to explore all our possible pursuits by limiting the set of decisions available to us.<sup>56</sup> Of course, it could be argued that this manipulation exists on an even more basic level through marketing techniques and political campaigns.

I contend that surveillance capitalism’s tactics constitute a clearer interference because of the opacity shrouding its tactics. Gerard uses the analogy of “black boxes” to refer to algorithms, implying that the sheer complexity and independence of the machine learning processes employed in surveillance capitalism leave users unaware of *how* they are being targeted or manipulated.<sup>57</sup> Users are generally aware of the persuasive intention behind marketing and campaigns, and can thus make their decisions with a certain degree of independence from this sort of interference. In the case of surveillance capitalism, the interference often occurs surreptitiously, leaving users little room to critically evaluate their decision-making process. This was also the case in the previously mentioned example of Facebook tracking mood changes to inform advertising tactics (see Introduction). Therefore, surveillance capitalism threatens the capabilities that individuals have reason to value, specifically, the capabilities for well-being and agency.

### *Section 2C: The Threat to Distributive Justice*

Lastly, surveillance capitalism harms social well-being by perpetuating distributive injustices. The primary concern that I will outline is the effect of surveillance capitalism on

---

<sup>56</sup>Henrik Skaug Saetra, “When Nudge Comes to Shove: Liberty and Nudging in the Era of Big Data,” *Technology in Society* 59 (November 1, 2019): 10, <https://doi.org/10.1016/j.techsoc.2019.04.006>.

<sup>57</sup>Gerards, “The Fundamental Rights Challenges,” 206

distributive justice. The exact effect that surveillance capitalism has on distributive justice is that it perpetuates unjust status inequalities. I take for granted that these unjust inequalities are harmful to society; whether these unjust inequalities constitute a sufficient harm to society is a debate that I will not broach. I will also not engage in a detailed description of the varying principles of distributive of justice; rather, I will focus on the theory of “equality of opportunity.”

The endorsement of some form of equality of opportunity is prevalent among distributive justice theorists.<sup>58</sup> Equality of opportunity requires that inequalities permitted by the general theory are only justified if people have the necessary kinds of opportunities to achieve greater or lesser amounts of goods.<sup>59</sup> Manovich argues that surveillance capitalism encroaches on equality of opportunity by dividing society into three “data-classes:” those who create data, those who collect data, and those who can analyze data.<sup>60</sup> The resultant data-class status hierarchy renders the first group – those who create data – subject to classification and profiling.

Since the logic of surveillance capitalism involves classifying individuals based on shared traits derived from data, algorithms can purposefully be designed to enable firms to engage in illegal forms of discrimination. For instance, while there is existing legislation outlawing discriminatory practices in the real estate industry, companies utilize Big Data models to identify and avoid advertising to potential property renters based on their racial background or socio-demographic status. These potential renters are identified through algorithms that sift

---

<sup>58</sup> Julian Lamont and Christi Favor, “Distributive Justice,” in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, (Metaphysics Research Lab, Stanford University 2017), <https://plato.stanford.edu/archives/win2017/entries/justice-distributive/>.

<sup>59</sup> There are multiple general theories of distributive justice amongst theorists. Here, I use “general theory” to refer expansively to the broad set of distributive justice theories that rely on the tenet of equality of opportunity.

<sup>60</sup> Manovich, Lev. “Trending: The Promises and the Challenges of Big Social Data,” In *Debates in the Digital Humanities*, ed. Matthew K. Gold (Minneapolis: University of Minnesota Press, 2012), <https://doi.org/10.5749/minnesota/9780816677948.003.0047>.

through “discrete online activity,” such as “liking things on Facebook.”<sup>61</sup> This example illustrates one of the most pernicious issues to do with surveillance capitalism: the “injustice of misrecognition” that creates unequal opportunities to access economic and social goods, eventually perpetuating unjust status inequalities.<sup>62</sup>

Furthermore, as alluded to in Section 2B, the new alternative data industry used in determining credit scores also exemplifies the injustices perpetuated by surveillance capitalism. Credit scores directly affect the opportunities afforded to individuals by determining financial and material circumstances in society. However, beyond the issues to do with capabilities, the logic of surveillance capitalism results in the production of *inaccurate* credit scores. Under surveillance capitalism, alternative data is used to contribute to these credit scores, however this alternative data often consists of the “vagaries of online identity” that can produce serious inaccuracies.<sup>63</sup>

This discussion of credit scores illuminates the severity of this issue: individuals may be unable to secure a loan, mortgage, or health insurance due to an incorrect assessment of their risk based on irrelevant data. In other words, surveillance capitalism often mischaracterizes and misrecognizes individuals to the point of limiting their opportunities in society. One could argue that addressing the algorithms to improve their accuracy might be the appropriate solution here. However, unlike the traditional mechanisms for determining credit scores, the logic of surveillance capitalism allows no mechanism for disputes or redress when mistakes occur. In this sense, the misrecognition of individuals can cause serious harms because there is no concrete

---

<sup>61</sup> Kate Crawford and Jason Schultz, “Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms,” *Boston College Law Review* 55, no. 1 (January 2014): 93, <https://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4>

<sup>62</sup> Jonathan Cinnamon, “Social Injustice in Surveillance Capitalism,” *Surveillance & Society* 15, no. 5 (December 2017): 615. <https://doi.org/10.24908/ss.v15i5.6433>.

<sup>63</sup> Cinnamon, “Social Injustice in Surveillance Capitalism,” 616.

way to address disputes. Individuals are afforded unequal access to opportunities based on inaccurate algorithms with no opportunity for resolution.

*Section 2D: On the universality of autonomy, freedom and distributive justice.*

Finally, I will consider whether surveillance capitalism constitutes a *global* harm. That is, are the tenets of autonomy, freedom and distributive justice valued cross-culturally such that a violation of these harms would be problematic on an international scale? I will answer this question on a case by case basis – arguing how each autonomy, freedom, and distributive justice all possess some degree of universal value.

To make an argument for the universality of autonomy as I have defined it, I will refer to Simon Caney’s argument for the universalism of certain values. Caney makes the case that certain morals that have universal form (in that the same principles apply) and universal scope (in that these principles apply to all). He justifies this using an argument he calls “The General Argument,” an argument predicated on two key premises:

1. The moral principles that apply to some persons apply to all persons who share some common morally relevant properties.
2. That people around the world share morally relevant similarities.<sup>64</sup>

Caney elaborates a defense of the second premise by arguing that persons throughout the world have common needs and vulnerabilities (i.e.: require food and shelter to survive, susceptible to disease) and common goods (i.e.: life, bodily health). I will not delve into a defense of Caney’s central assumption, rather, I will consider his subsequent claim: based on these universal moral

---

<sup>64</sup> Simon Caney, “Universalism,” in *Justice Beyond Borders* (Oxford: Oxford University Press, 2005), <https://doi.org/10.1093/019829350X.003.0002>.

values, there are universal principles of civil and political justice, the right to autonomy being among them.

One of the justifications of universal civil and political rights, termed the “well-being argument,” is that such rights are necessary for human beings to flourish. Caney contends that the claim for agency as a right essential to human well-being is a “familiar one,” specifying agency as “being in charge of one’s own life and making one’s own decisions.”<sup>65</sup> Though Caney refers to this property as agency, I would argue that the language used to describe agency bears strong similarity to my earlier discussion of autonomy; especially as the emphasis on “making one’s own decisions” seems analogous to making one’s own choices without external interference, and to Grafanaki’s definition of autonomy as self-determination and independent decision-making.

While one might think that agency is a parochial western value, Caney emphasizes that the universality of such a value can be found in a multitude of non-western cultures: Buddhists, for instance, strongly emphasize the need for individuals to acquire independence through their own reflection and action. Furthermore, Ghanaian philosophers like Kwame Gyekye and Kwasi Wiredu argue that some African traditions of thought also stress the value of individuality and independence.<sup>66</sup> There is also evidence for moral autonomy in other non-western, less individualistic societies – Joseph Chan makes the argument that there is a conception of moral autonomy in Confucian (the grounding philosophy of Chinese government and society) ethics that supports, to a certain degree, the independence of choice and actions from external factors or

---

<sup>65</sup> Simon Caney, “Civil and Political Justice,” in *Justice Beyond Borders* (Oxford: Oxford University Press, 2005), <https://doi.org/10.1093/019829350X.003.0003>.

<sup>66</sup> See above.

coercion.<sup>67</sup> This literature tells us that there is good reason to think that autonomy, to some degree, is a universal value that holds weight across different cultures.

In a similar vein, can we consider the claim that individuals should have the freedoms to pursue the capabilities they value as being universally accepted? It is significant to note that the epistemological intent behind Sen's theory already imbues the notion of capabilities with some degree of cross-cultural value. Sen developed this approach "in order to identify a space in which we can make cross-cultural judgments on the quality of life."<sup>68</sup> The capability approach takes account of human diversity in around three ways, two of which are relevant to my discussion.

This approach encompasses a wide-range of dimensions in conceptualizations of well-being and distinguishes well-being freedom from agency freedom, allowing for a diversity of activities to be encompassed under capabilities.<sup>69</sup> It is therefore plausible that cross-cultural variances in what constitutes well-being may be accounted for under this theory. Similarly, the inclusion of agency freedom allows for pursuits that are not be integral to well-being to be considered under the capabilities approach. Therefore, even if different countries define well-being in various ways, a pursuit that does not fall under well-being may still be considered essential to a person's substantive freedom.

The capabilities definition of freedom, therefore, allows for universal and cross-cultural validity. One might be concerned with the limitations surveillance capitalism places on specific capabilities, and ask whether those specific capabilities are considered universal. I contend that the capability to take out loans, to have employment, and to be insured are ones that are valued in

---

<sup>67</sup> Joseph Chan, "Moral Autonomy, Civil Liberties, and Confucianism," *Philosophy East and West* 52, no. 3 (2002): 281–310, <http://www.jstor.org/stable/1400320>

<sup>68</sup> Chad Kleist, "Global Ethics: Capabilities Approach," in *Internet Encyclopedia of Philosophy*, accessed March 27, 2022, <https://iep.utm.edu/ge-capab/>.

<sup>69</sup> Robeyns and Byskov, "The Capability Approach."

most nations (exempting perhaps indigenous tribes). Furthermore, the evidence for freedom of expression being valued to some degree globally (see Section 2B) substantiates the claim that this capability is somewhat universally valued. There will of course be variations as to the extent that different nations value capabilities, but for the sake of my argument, it is sufficient to establish that the capabilities approach holds basic universal value, and that surveillance capitalism threatens certain capabilities that are valued transnationally.

Lastly, how might we establish distributive justice, or more specifically, the equality of opportunity as a universal value? Gillian Brock writes that “the ideal of fair equality of opportunity is widely endorsed as a central commitment within liberal democracies.”<sup>70</sup> But what about nations or communities that are not liberal democracies? I confess that in illiberal democracies (such as Singapore or China) or authoritarian regimes (like Saudia Arabia), there is not much evidence to suggest that these nations give normative weight to the equality of opportunity (at least with regards to political organization and societal distribution). That being said, as Caney argues, we should not conflate the views of the political elite with their peoples.<sup>71</sup> It is possible that citizens of such countries might value equality of opportunity even if it is not central to their society’s organization. This is entirely a speculative claim, and requires more investigation on citizens attitudes towards specific liberal tenets within countries that do not identify as liberal democracies.

Additionally, there is research that demonstrates elements of egalitarianism and equality of opportunity in Confucianism.<sup>72</sup> There is also academic research theorizing egalitarian

---

<sup>70</sup> Gillian Brock, “Equality of Opportunity and Global Justice,” in *The Oxford Handbook of Global Justice*, ed. Thom Brooks (Oxford: Oxford University Press, 2020), <https://doi.org/10.1093/oxfordhb/9780198714354.001.0001>.

<sup>71</sup> Caney, “Civil and Political Justice.”

<sup>72</sup> Ruiquan GAO and Xin YAN, “The Source of the Idea of Equality in Confucian Thought,” *Frontiers of Philosophy in China* 5, no. 4 (2010): 486–505, <http://www.jstor.org/stable/40981115>

elements and a general conception of the fundamental equality of all persons in Islamic texts.<sup>73</sup> While this body of literature vaguely gestures at the normative value of equality (I would not go so far as to contend that the exact interpretation of equality of opportunity as I have presented it appears verbatim), there is no overwhelming evidence to indicate that equality of opportunity is valued at the international level. This is a valid objection to my argument; however, I will continue to refer to surveillance capitalism's threats to distributive justice, because I assume that these harms would be unacceptable to the numerous nations that are liberal democracies or value equality of opportunity.

### **Section 3: Exploring Current Conceptions of Data Ownership and Privacy**

Having established the basic tenets of this practice, and outlining the possible harms and threats to users, I now seek to answer the question: what is currently being done to mitigate the negative impacts of surveillance capitalism? First, it is necessary to define the scope of protections being examined, i.e., should we look to domestic or international law? I will establish that it is necessary to look at international laws and regimes, largely because the internet and associated "cyberspace" often transcends national borders.

#### *Section 3A: Justifying Data Protections at the International Level*

Zuboff's scholarship specifically focuses on the practices of Google, Facebook, and Microsoft: corporations she identifies as being firmly embedded in the logic of surveillance capitalism.<sup>74</sup> While she mentions that Amazon is migrating towards surveillance capitalist tactics, and that Apple has, as of 2018, drawn the line, these corporations are not included in her

---

<sup>73</sup> Noah Feldman, "Political Equality and the Islamic State," *Philosophical Topics* 30, no. 2 (2002): 253–72, <http://www.jstor.org/stable/43154401>

<sup>74</sup> Zuboff, *The Age of Surveillance Capitalism*, 22.



analysis.<sup>75</sup> Nevertheless, the three corporations she analyzes are all multinational and operate in a number of territories around the world; Google alone has operations in 219 countries.<sup>76</sup> This indicates that an international framework may be well poised to address harms generated by firms engaging in surveillance capitalism. Moreover, the internet consists of “cyberspace,” an amorphous “virtual” world created by the components of the Internet’s infrastructure.<sup>77</sup> Security experts consider cyberspace to be part of the “global commons,” a region outside the territorial jurisdiction of any state, much like the high seas, airspace and outer space.<sup>78</sup> The physical structure of cyberspace, which includes computer servers, cables, and other equipment, is also dispersed across the planet. So, the nature of cyberspace necessitates an examination of international regulations.

Of course, it is possible for states to tightly regulate the internet at the domestic level; countries like China, Vietnam, and Burma/Myanmar exemplify this.<sup>79</sup> Without endorsing the restrictive elements of the systems themselves, these examples substantiate the claim that states can control the internet within their territory. However, the presence of international regulation increases the possibility for cross-territorial claims of data breaches, which may be uniquely relevant to addressing the harms generated by surveillance capitalism. Jonathan Cinnamon notes that “the territoriality of personal data accumulation means that if you live outside of the data center’s political jurisdiction, it is likely that a foreign entity is controlling your data, which means that you’ll be severely restricted from making a justice claim regarding access, the ways

---

<sup>75</sup> Zuboff, *The Age of Surveillance Capitalism*, 44.

<sup>76</sup> David Goldman, “Google: The Reluctant Censor of the Internet,” *CNN*, January 4, 2015, <https://money.cnn.com/2015/01/04/technology/google-censorship/index.html>.

<sup>77</sup> Jennifer Bussell, “Cyberspace,” in *Encyclopedia Britannica*, March 12, 2013, <https://www.britannica.com/topic/cyberspace>.

<sup>78</sup> Ronald J Deibert, and Masashi Crete-Nishihata. “Global Governance and the Spread of Cyberspace Controls,” *Global Governance* 18, no. 3 (2012): 345, <http://www.jstor.org/stable/23269961>.

<sup>79</sup> Barney Warf, “Geographies of Global Internet Censorship,” *GeoJournal* 76, no. 1 (2011): 8, <http://www.jstor.org/stable/41148433>

your data are used or how it represents you.”<sup>80</sup> Domestic laws in isolation would be unable to address such supranational claims. To provide an overarching sense of domestic data protection policies, I will outline generalized models that exist amidst different countries but will refrain from providing a piecemeal analysis specific to each region.

### *Section 3B: Surveying the Landscape of Data Privacy*

Currently, most of the legal discourse surrounding the effects of surveillance capitalism is firmly entrenched in a discussion of privacy. Modern conceptions of the right to privacy often draw inspiration from Article 12 of the Universal Declaration of Human Rights, which states:

“No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.”<sup>81</sup>

According to David Banisar and Simon Davies, the interest in the right to data privacy increased in the 1960s and 70s, around the same time ARPANET and Internet-based technologies were taking off.<sup>82</sup>

The first data protection law in the world was enacted in Germany in 1970; throughout this decade, similar national laws were enacted in other parts of the Western world including Sweden, the United States, Germany, and France.<sup>83</sup> From this legislation, two crucial international instruments evolved. First, the Council of Europe’s (COE) 1981 “Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data,” which

---

<sup>80</sup> Cinnamon, “Social Injustice in Surveillance Capitalism,” 617.

<sup>81</sup> United Nations. “Universal Declaration of Human Rights.” United Nations. Accessed November 21, 2021. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.

<sup>82</sup> David Banisar, and Simon Davies, “Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments,” *UIC John Marshall Journal of Information Technology & Privacy Law* 18, no. 1 (January 1999): 10. <https://repository.law.uic.edu/jitpl/vol18/iss1/1>.

<sup>83</sup> See above.

has been adopted by over 20 countries and signed by another 6 nations. The second is the Organization for Economic Cooperation and Development's (OECD) "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data," which has been referenced in the national legislation of non-OECD countries.<sup>84</sup> Banisar and Davies posit that the content of these two documents form the backbone of the data protection laws in dozens of countries. Generally speaking, the declaration and laws across varying countries require that personal information must be:

- Obtained fairly and lawfully
- Used only for the original specified purpose
- Adequate, relevant, and not excessive to purpose.
- Accurate and up to date.
- Accessible to the subject.
- Kept secure, and
- Destroyed after its purpose is completed.<sup>85</sup>

Additionally, Banisar and Davies' survey of international privacy models identifies four broad classes of privacy protection:

1. Comprehensive laws: In regions like Europe, countries have a general data protection law that oversees the collection, use, and dissemination of personal information in the public and private sectors. Most of these countries have appointed an official or agency to oversee enforcement. However, the powers of enforcement vary greatly by country and can be affected by resource limitations.

---

<sup>84</sup> Banisar and Davies, "Global Trends in Privacy Protection," 10.

<sup>85</sup> Banisar and Davies, "Global Trends in Privacy Protection," 11.

2. Sectoral laws: In lieu of general data protection rules, countries like the United States have specific sectoral laws. Enforcement is achieved through a wide range of tactics. This approach necessitates that new legislation be introduced with every new technology, which leads to gaps in existing laws.
3. Self-regulation: Countries like Japan and Singapore allow companies and industry bodies to self-regulate by establishing codes of practice. Due to inadequacy in these industry codes and no enforcement power, this approach falls short of the data protection laws in other countries.
4. Technologies of privacy: Users of the internet and other physical applications employ programs and systems that ensure data privacy, such as encryption, anonymous remailers, and proxy servers.<sup>86</sup>

Despite the presence of data privacy laws at an international and regional level, the wide variations in established approaches and efficacy leaves significant lacunae in protections that surveillance capitalism can seep through. These gaps persist even in regions that are moving towards stronger data protection laws.

Some countries are taking steps to match the burgeoning threat that surveillance capitalism poses. In December 2020, the European Commission proposed the Digital Services Act and the Digital Markets Act, putting forward a comprehensive set of new rules for online platforms that operate in the European Union.<sup>87</sup> The proposals were created with an acknowledgement of the newer mechanisms and tactics employed by tech giants to gather and repurpose data, and are therefore perhaps uniquely situated to address surveillance capitalism's

---

<sup>86</sup> Banisar and Davies, "Global Trends in Privacy Protection," 14.

<sup>87</sup> Isabel Teixeira, "Digital Markets Act: Ending Unfair Practices of Big Online Platforms," European Parliament, November 23, 2021, <https://www.europarl.europa.eu/news/en/press-room/20211118IPR17636/digital-markets-act-ending-unfair-practices-of-big-online-platforms>.

threats.<sup>88</sup> Specifically, the DMA aims to fill the current gaps in the GDPR (EU General Data Protection Regulation) in addressing data-collection. Depending on how it is enacted, the DMA could limit the granularity and comprehensiveness of datasets or UPIs compiled by firms like Facebook and Google.<sup>89</sup> Specifically, Article 5(a) prohibits “gatekeepers,” (online platforms with at least 45 million monthly active users) from “combining personal data,” without the active consent of end-users, limiting platforms’ ability to build UPIs.<sup>90</sup>

Broadly speaking, the DMA prioritizes transparency objectives in behavioral data collection and advertising, rather than focusing on the regulation of this data collection. This is problematic, because “transparency” often involves privacy policies, terms-of-service agreements, and other informative endeavors that users regularly bypass. An empirical study of privacy policy and terms of service reading behavior found that 74% of users skipped reading the policies and opted for the “quick-join” clickwrap to save valuable time.<sup>91</sup>

This phenomenon sheds light on a larger issue with data privacy laws: typically, these regulations can be circumvented through an offering of a “contract,” that users blithely accept. Zuboff refers to these contracts as “euphemisms of consent,” because users typically accept them without any critical thought, and furthermore, because surveillance capitalist rendition tactics transcend the conventions of “opting in” and “opting out.”<sup>92</sup> Since surveillance capitalist

---

<sup>88</sup> Scientific Foresight, “Surveillance Capitalism and Europe’s Moral Duty to Shape a Human-Centric Digital Future,” European Parliamentary Research Service, January 14, 2021, <https://epthinktank.eu/2021/01/14/surveillance-capitalism-and-europes-moral-duty-to-shape-a-human-centric-digital-future/>.

<sup>89</sup> Julian Jaurisch and Aline Blankertz, “What the European DSA and DMA Proposals Mean for Online Platforms,” *Brookings* (blog), January 14, 2021, <https://www.brookings.edu/techstream/what-the-european-dsa-and-dma-proposals-mean-for-online-platforms/>.

<sup>90</sup> “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Contestable and Fair Markets in the Digital Sector (Digital Markets Act),” European Union Law, Eur-Lex, accessed December 22, 2021, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN>.

<sup>91</sup> Jonathan Obar and Anne Oeldorf-Hirsch, “The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services,” *Information, Communication & Society* 23 (July 2018): 14. <https://doi.org/10.1080/1369118X.2018.1486870>.

<sup>92</sup> Zuboff, *The Age of Surveillance Capitalism*, 374.

practices overtly flaunt existing regulations and can bypass very progressive iterations of privacy law, there is a need for a different approach to combating surveillance capitalist tactics.

#### **Section 4: Justifying the Right to Data as a Human Right**

I will now defend the following central claim: that the issue of surveillance capitalism can be better remediated by establishing that an individual's right to the data they generate should be encompassed by the *human right to property*. There are two thresholds to this argument: first, I must establish that the right to data should be a human right. This premise is not specific to property; rather, I intend to establish that either through privacy or property, every individual has a "human right to data." To do so, I will utilize the institutional lens of human rights to describe how the right to data should be encompassed by the larger body of human rights, referencing the works of John Rawls, Charles Beitz, and Joseph Raz.

The second threshold is establishing that data should be conceived of, at least in part, as property. Since I am utilizing the right to data as a means of mitigation for surveillance capitalism, I will argue that construing data as property addresses the previously established harms from surveillance capitalism (see Section 2). At this point, I will address relevant objections, namely the suggestion that user-generated data would be better protected by a regime of privacy rather than a property rights framework. In the following analysis, I will use the term "data" to broadly reference the digital exhaust I referenced in Section 1, that is, the collateral data generated by a user while interacting with the internet *before* it is put through machine learning processes to create the "prediction products" that companies use to target consumers.

#### *Section 4A: Grounding the Political Conception Argument for Human Rights*

The “political conception” argument functions as answers to the question “What are human rights?” and “What makes them distinct from other rights?” If I can establish that the right to data meets the conditions set forward by the political conception theory, then I can argue that it is fundamentally a human right. To make this claim, I will first briefly describe the distinction between the naturalistic and political conception of human rights. The naturalistic conception of human rights draws from the writings of Hugo Grotius, Samuel von Pufendorf and John Locke. This conception holds that human rights are “rights that all human beings possess simply in virtue of their humanity, and which can be identified simply by the use of ordinary moral reasoning [natural reason].”<sup>93</sup> Evidently, the naturalistic argument is grounded in morality, because it presupposes that these rights are “pre-legal,” and arise independently of the state.

However, works by contemporary philosophers such as John Rawls, Charles Beitz, and Joseph Raz gave significant impulse to an alternative view: the political conception of human rights. Advocates of this conception generally argue that the distinct nature of human rights is conveyed through their role or function in modern international political practice. However, there are varying interpretations of the conditions necessitated by the political conception. While the views espoused by Rawls, Beitz and Raz share many commonalities, I also will highlight the non-overlapping conditions between these views. Subsequently, if I can demonstrate that the human right to data meets both the common and unique (to each view) conditions for the political conception, I will have established that there is a human right to data at a more rigorous level that would be achieved by adhering to just one of these views.

---

<sup>93</sup> Rowan Cruft, Matthew S. Liao, and Massimo Renzo, *Philosophical Foundations of Human Rights*. Philosophical Foundations of Law (Oxford: Oxford University Press, 2015): 4, <https://doi.org/10.1093/acprof:oso/9780199688623.001.0001>.

Rawls claims that human rights are a “special class of rights designed to play a special role in a reasonable law of peoples for the present age.”<sup>94</sup> He was interested in a narrow set of *international* human rights that were defined by the role they played in clarifying other normative concepts, such as the legitimacy of a regime and its legal order, sovereignty, the permissible grounds for intervention, and the limits to moral pluralism. Since Rawls’ original paper, his claim has been reiterated and extended by several scholars.

This includes Charles Beitz who posits a broader “practical conception” of human rights. Beitz expresses that human rights are not solely defined by the narrow roles Rawls prescribed, but rather encompass guiding practical judgements about international responsibility or concern.<sup>95</sup> Beitz specifies that human rights are rights whose object is to “protect urgent individual interests against certain predictable dangers to which they are vulnerable under typical circumstances of life in a modern world order composed of states.”<sup>96</sup> In a similar vein, Joseph Raz’s account of human rights expands the definition to include rights that can be held against international agents and organizations of all sorts, not just states.<sup>97</sup>

Raz also highlights that in the context of human rights, the limits of sovereignty cannot be conflated with the limits of legitimate authority. At this point, I will highlight a key difference between Rawls and Raz’s arguments, primarily to establish that Raz suggests a more stringent standard for the justifiability of intervention. In the subsequent analysis, I will use Raz’s standard to bolster the strength of my argument. Both Rawls and Raz agree that human rights are rights

---

<sup>94</sup> John Rawls, “The Law of Peoples,” *Critical Inquiry* 20, no. 1 (Autumn 1993): 58, <http://www.jstor.org/stable/1343947>.

<sup>95</sup> Charles R. Beitz, *The Idea of Human Rights* (Oxford: Oxford University Press, 2009), <https://doi.org/10.1093/acprof:oso/9780199572458.001.0001>.

<sup>96</sup> Beitz, *The Idea of Human Rights*, 109.

<sup>97</sup> Joseph Raz, “Human Rights Without Foundations,” *Oxford Legal Studies Research* (January 2007), [https://scholarship.law.columbia.edu/faculty\\_scholarship/1491](https://scholarship.law.columbia.edu/faculty_scholarship/1491).



that effectively “disable” a state’s sovereignty. This means that if a state violates human rights, and another state chooses to interfere, the original state cannot invoke sovereignty as a defense. However, Rawls’ original account claims that human rights are “necessary conditions of any system of social-cooperation,” where social cooperation is a “productive and socially coordinated activity” that yields mutual advantages to all the parties involved.<sup>98</sup>

On the other hand, Raz contests the association between the conditions of social cooperation and the limits of sovereignty. According to Raz, the scope of a state’s authority cannot be curtailed by the degree to which a state is internally acting in a “socially cooperative” manner, because the moral principles which govern social relations and a society’s structure varies across communities. A state’s internal political order may not live up to Rawlsian standards for social cooperation, but this does not mean that this state is in violation of human rights and requires external intervention.

A synthesis of these scholar’s viewpoints can be constructed in the following way:

- 1: Human Rights are a special class of rights designed to play a special role in international law.
- 2: Rights are human rights when their fulfillment is a necessary condition of the legitimacy of a regime and the decency of its legal order, and when they set limits to moral pluralism. Moral pluralism can be thought of as a diversity of moral viewpoints that cannot be reconciled with another but all possess validity.<sup>99</sup> Therefore, a human right must constrain this pluralism by reinforcing a moral doctrine that is not up for debate.

---

<sup>98</sup> John Rawls, *The Law of Peoples: With “The Idea of Public Reason Revisited”* (Cambridge: Harvard University Press, 2001): 68, <https://doi.org/10.2307/j.ctv1pncngc>.

<sup>99</sup> Leif Wenar, “John Rawls,” in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Summer 2021 (Metaphysics Research Lab, Stanford University, 2021), <https://plato.stanford.edu/archives/sum2021/entries/rawls/>.

3: Rights are human rights when violations of these rights provide permissible grounds for intervention and disable the boundaries of state sovereignty.

4: The moral limits of state sovereignty are not determined by the internal social cooperation of a political order, but also depend on the justifiability of interference by others.

5: The broad mandate or object of human rights is to “protect urgent individual interests against certain predictable dangers to which they are vulnerable under typical circumstances of life in a modern world order composed of states.”<sup>100</sup>

Importantly, in adhering to the political conception argument, I am not attempting to claim that an individual’s right to data is morally justified as a human right. Rather, I contend that based on an interpretation of the normative principles underlying the international human rights practice as we know it, there is a set of conditions that define what a human right is. According to the political conception, then, an adequate theory of human rights will be grounded in an interpretation of the current practice of human rights.

This might lead to the following sort of concern: I may have established that there is a human right to data by satisfying the criteria set forth by an interpretation of the current human rights practice, but there is nothing intrinsically *special* about the human rights practice. If the practices of the existing human rights practice were to change, so would the principles flowing from it, therefore invalidating my entire analysis. Since I cannot normatively justify the human right to data, and can only justify it in terms of the existing human rights corpus and associated principles, one might consider the practice based conception to be weak grounds for my argument for the human right to data.

---

<sup>100</sup> Beitz, *The Idea of Human Rights*, 109.

To address the concern that there is nothing intrinsically special about the human rights practice, I will briefly digress into Ronald Dworkin's account of "constructive interpretation."<sup>101</sup> Dworkin originally synthesized his theory of constructive interpretation in reaction to positivist conceptions of law, however, I refer to his argument as it applies to my analysis. He proposes two assumptions about existing practices: first, that a practice does not simply exist, but has some intrinsic value in serving some interest or enforcing a principle that exists separate to the practice itself. Second, that the practice as it exists now does not necessarily *per se* serve the underlying interest, purpose, or principle, and thus can be interpreted differently.<sup>102</sup>

Under this constructivist account, the issue with the practice-based justification is resolved. This is because we can assume that the human rights practices in place serve some intrinsic value or enforce a set of principles that are entirely distinct to the practice itself. For instance, we could posit that the specific human right of freedom from torture is valuable in ensuring some overarching principle of treating humans with dignity or kindness. In connection to my argument, we might think that if the existing human rights practice affirms some overarching value of granting individuals autonomy or equality, then the human right to data would ultimately serve that pre-existing intrinsic value.

Importantly, as Andrea Sangiovanni points out, these "first principles" aren't affirmed as self-evident, their justification ultimately "flows from their place in the whole picture."<sup>103</sup> Furthermore, the second principle allows us to understand why a political conception of human rights does not justify whatever the actual practices happen to be. These actual practices are

---

<sup>101</sup> Francisca Christina Wilhelmina de Graaf, "Dworkin's Constructive Interpretation as a Method of Legal Research.," *Law and Method*, no. 12 (2015), <https://doi.org/10.5553/REM/000012>.

<sup>102</sup> See above.

<sup>103</sup> Andrea Sangiovanni, "How Practices Matter," *Journal of Political Philosophy* 24, no. 1 (March 2016): 11, <https://doi.org/10.1111/jopp.12056>.

ultimately responsive to principles that are imminent in them, but they need not necessarily live up to these principles. Therefore, a constructive interpretation of a practice provides room for the criticism of existing practices, while still allowing us to justify human rights using the political conception.

#### *Section 4B: Establishing the Right to Data as a Human Right*

Having broadly synthesized differing accounts of the political conception, I now intend to show that an individual's right to data meets the non-overlapping criterion established by these different theories. The initial three criteria stem from Rawlsian theory. While Joseph Raz accepts the first three basic assumptions, he contests Rawls' claim that intervention stems from internal social cooperation and provides a more specific requirement about the justifiability of interference.<sup>104</sup>

Raz's disagreement with Rawls is the basis for the fourth criterion mentioned in Section 4A. So, at this stage, I will address this disagreement and demonstrate that the right to data meets Raz's more stringent justifiability of interference condition. Lastly, I will discuss the fifth criterion, which comes from Beitz's argument. Beitz accepts Rawls' general principles, but argues that his approach is too narrow. He characterizes human rights as addressing "dangers" to the common individual – this discussion will lead us into the next section, where I argue that classifying data as property is the appropriate form of redress for these dangers.<sup>105</sup>

Given that the first point is a general point about the nature of human rights, I will proceed with an analysis of the second criterion. First, I need to establish that the right to individual data is a necessary condition of the legitimacy of a regime and the decency of a legal

---

<sup>104</sup> Raz, "Human Rights Without Foundations," 13.

<sup>105</sup> Beitz, *The Idea of Human Rights*, 109

order. Here, the analysis of political legitimacy becomes slightly convoluted because political legitimacy is often defined by the exercise of civil and political rights by citizens that justify political authority. A perceptive reader will note that given my earlier reliance on legitimacy to explain human rights, turning now to rights to explain legitimacy may result in a circular argument. However, to continue appealing to the framework I have established, I will have to reference Rawls' own definition of political legitimacy. Therefore, while this argument may seem circular, I contend that the circularity is virtuous in that it allows for cohesion with the pre-established framework.

In the following section, I will be using Rawls' definition of political legitimacy because the criterion pertaining to political legitimacy is from Rawls' work. According to Silje A. Langvatn, Rawls provides several characterizations of political legitimacy:

1. Legitimacy requires both sufficient procedural justice and sufficient outcome justice. Procedural justice refers to the justice of the procedure that determines how benefits and burdens are allocated to individuals, while outcome justice refers to the justice of the final allocation itself.<sup>106</sup>
2. Legitimacy connects to the pedigree of those who have political authority and a law or institution came about i.e. whether political officials, laws, and institutions came into office/arose in accordance with established rules and traditions.<sup>107</sup>

Rawls' characterization of legitimacy also distinguishes between justice and legitimacy: a law may be just in that it produces fair outcomes, but may be politically illegitimate because the law has been created in a process that is not sufficiently just. Furthermore, he differentiates

---

<sup>106</sup> David Miller, "Justice," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Fall 2021 (Metaphysics Research Lab, Stanford University, 2021), <https://plato.stanford.edu/archives/fall2021/entries/justice/>.

<sup>107</sup> Silje A. Langvatn, "Legitimate, but Unjust; Just, but Illegitimate: Rawls on Political Legitimacy," *Philosophy & Social Criticism* 42, no. 2 (February 2016): 134, <https://doi.org/10.1177/0191453715615386>.

between “the legitimacy of political institutions and the legitimacy of decisions and as enacted pursuant to them; and also between accepting a constitution as legitimate and accepting as legitimate a particular statute or decision in accordance with the constitution.”<sup>108</sup> An important caveat is that this perception of political legitimacy would not account for monarchical, authoritarian, or overly corrupt governments where outcome or procedural justice would not be of much concern.

When users do not have rights to their data, as is the status quo under surveillance capitalism, political legitimacy as characterized by Rawls may be undermined. First, surveillance capitalism threatens to disrupt the outcome justice of decisions enacted by political institutions. As mentioned in Section 2C, surveillance capitalism can result in unfair outcomes by allowing real-estate companies to bypass anti-discrimination laws established by the legislature.

There is also evidence of surveillance capitalism concretely affecting the process through which political officials come into office, evidenced by the highly publicized Cambridge Analytica case. The now-defunct political data organization, in collaboration with Facebook, illicitly collected the data of millions of people to influence voting choices during the 2016 U.S Presidential Campaign and the 2016 Brexit referendum.<sup>109</sup> As such, the U.S Presidential Office and Brexit referendum did not arise in accordance with established rules and traditions – specifically, the established traditions that are relevant to a fair democratic process.

Regarding the second part of this criterion, we must now turn to whether the right to one’s data sets limits to moral pluralism. Rawls contextualizes moral pluralism by describing human rights as of “universal application” and “hardly controversial in their general

---

<sup>108</sup> Langvatn, “Legitimate, but Unjust; Just, but Illegitimate,” 134.

<sup>109</sup> Hern, “Cambridge Analytica.”

intention.”<sup>110</sup> In this sense, he claims, they specify the “outer boundary of admissible domestic law.”<sup>111</sup> This specific condition was conceived in part as an answer to the cross-cultural validity argument that is often used by detractors of the international human rights regime, because it defines human rights as being the product of consensus between cultures rather than arising primarily from a Western conception of morality. For the sake of our argument, we must consider whether the right to data is hardly controversial in its general intention, and whether this right may be applied universally. I postulate that the sheer existence of transnational internet privacy laws (see Section 3B) indicates that the individual right to data is somewhat globally accepted, even if the actual efficacy of these laws is questionable.

The new European legislation on the horizon (see Section 3B) also indicates a growing consensus on establishing rights over personal data generated on the internet. The emergence of increasingly stringent data protections laws is not restricted to Western nations: on August 20, 2021, the Standing Committee of China’s National People’s Congress promulgated the Chinese Personal Information Protection Law (PIPL) which aims to “protect the rights and interest of individuals,” “regulate personal information processing activities,” and “facilitate reasonable use of personal information.”<sup>112</sup>

Furthermore, in June 2014, the African Union (AU) adopted the AU Convention on Cybersecurity and Data Protection, which recognizes the “urgent need to establish a mechanism to address the dangers and risks deriving from the use of electronic data and individual records, with a view to respecting privacy and freedoms.”<sup>113</sup> Article 8 of this convention states that the

---

<sup>110</sup> Rawls, “The Law of Peoples,” 59.

<sup>111</sup> See above

<sup>112</sup> Xu Ke et al., “Analyzing China’s PIPL and How It Compares to the EU’s GDPR,” *Nternational Association of Privacy Professionals* (blog), August 24, 2021, <https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/>.

<sup>113</sup> “African Union Convention on Cyber Security and Personal Data Protection,” African Union, June 27, 2014, <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>.

established objective of the convention shall “ensure that any form of data processing respects the fundamental freedoms and rights of natural persons.”<sup>114</sup> Though this convention has not yet been ratified by 15 out of the 54 AU member jurisdiction, it provides a data protection framework which might be reflected in national legislations across Africa, and also substantiates an emerging global recognition of the need for rights to personal data.<sup>115</sup>

With regards to public opinion itself, though there is a lack of cross-cultural studies that examine public perception of personal data, an empirical study of participants from Germany, Great Britain, and the United States found that respondents overwhelmingly object to the collection and use of sensitive personal information and to the personalization of political campaigning.<sup>116</sup> An important reservation here is that academic studies typically frame the right to data as a negative right (the right to *not* have data collected) rather than the right to individual data itself; the impact of question framing in this context is not a question I will address, but one that requires more attention. A possible objection to this argument is that the global disparities in access to the Internet or technology (i.e: “the digital divide”) undermines the global applicability of the right to data. However, if states are moving *towards* improved technological access, as is indicated by a 2018 UN General Assembly Resolution, then it is fair to assume that the right to individual data may soon become a universal issue.<sup>117</sup>

---

<sup>114</sup> “African Union Convention on Cyber Security and Personal Data Protection.”

<sup>115</sup> Dean Chivers, “Personal Data Protection in Africa” (Deloitte, 2017), <https://www2.deloitte.com/za/en/pages/risk/articles/personal-data-protection-in-africa.html>.

<sup>116</sup> Anastasia Kozyreva et al., “Public Attitudes towards Algorithmic Personalization and Use of Personal Data Online: Evidence from Germany, Great Britain, and the United States,” *Humanities and Social Sciences Communications* 8, no. 1 (May 14, 2021): 1–11, <https://doi.org/10.1057/s41599-021-00787-w>.

<sup>117</sup> “Second Committee Approves 12 Resolutions, Including Texts on Eradicating Rural Poverty, Addressing Digital Divide,” United Nations, November 30, 2018, <https://www.un.org/press/en/2018/gaef3511.doc.htm>.



Next, we must address whether a violation of the right to data is justified grounds for international intervention. Importantly, I note that by “intervention” I do not imply armed or militaristic styles of intervention; rather, as I will establish in the subsequent paragraph using Beitz’s argument, I take “intervention” to include a broader range of non-coercive political and economic measures. The very nature of surveillance capitalist logic and the structure of the corporations that deploy these tactics necessitates international intervention. As discussed in Section 3A, the internet often transcends sovereign boundaries, as do the operations of several major internet-based corporations.

Cyberspace is explicitly recognized as part of a region known as the international commons, as such, any regulations or rights over the products generated in cyberspace must exist both within and outside state borders. For instance, activist Max Schrems took legal action against Facebook Ireland when it was discovered that the company was exporting data to its US-based parent company.<sup>118</sup> This case highlights how data and behavioral insights may be exported or transferred internationally, which is why the right to data must be established at a level superseding sovereign boundaries.

An objection to this argument might take the following form: if the United States has established that corporations *can* mine and collect behavioral data, through a lack of explicit regulations or laws, would the presence of a right to individual data be grounds for another country to intervene? The thought here is that the United States’ violation of the right to data is not sufficient grounds for external intervention. This objection bears strong similarity to Raz’s

---

<sup>118</sup> “Data Protection Commissioner v. Facebook Ireland Ltd.,” *Harvard Law Review* 134, no. 4 (February 2021), <https://harvardlawreview.org/2021/02/data-protection-commissioner-v-facebook-ireland-ltd/>.

primary concern with Rawl’s theory of human rights, in that a State can exceed its legitimate authority (or violate its “internal social cooperation”) without justifying external intervention.

As a means of responding to the aforementioned objection, and addressing the fourth criterion, I will now discuss the justifiability of interference condition. Raz’s notion of justifiable interference is a more stringent standard for human rights than Rawls’ original condition, which simply holds that a human right must justify disabling boundaries of state sovereignty. I am introducing this specific argument from Raz to suggest that even if held to Raz’s more rigorous standard, the right to data is still justified. Raz posits that a state’s right to non-interference is not solely dependent on its internal social cooperation, rather, it is also contingent on the justifiability of interference itself. With respect to the aforementioned objection, the individual right to data would not provide justifiable grounds for external interference.

However, the right to data would surely provide grounds for *specific* external intervention. If the United States was allowing corporations to mine and extract the behavioral data of citizens of the United Kingdom, then the right to data would provide reasonable grounds for the United Kingdom to intervene. Furthermore, as Beitz suggests, there is a broad range of non-coercive political and economic measures that could constitute intervention – as such, the role of human rights need not be solely restricted to the *pro tanto* justification of foreign interference.<sup>119</sup> With regards to the hypothetical scenario, the United States actions’ may be grounds for sanctions or official rebuke even if they are not subject to armed intervention.

The fifth and last premise is based on Beitz’s broader conception of the role of human rights. Beitz implies a set of guiding practical judgements about international responsibility or concern, namely, protecting individuals against certain typical dangers that are commonplace in

---

<sup>119</sup> Beitz, *The Idea of Human Rights*, 109

a modern world made up of States. Therefore, the question that needs to be answered is whether the right to data protects individuals against certain typical, commonplace dangers. As previously established, surveillance capitalism poses a multitude of dangers to the common individual, and due to the nature of cyberspace, is a distinctively *international* matter of concern. Hence, the individual right to data to their own data generated meets the general criterion and definitions for what constitutes a human right.

### **Section 5: Justifying the Right to Data Under a Property Framework**

In Section 4B, I established that the right to data, in some shape or form, should constitute a human right under the political conception of human rights. Now, I will advance the argument that the right to data should take the form of a property right. I will begin by explaining the pre-existing basis for property rights within the human rights corpus in Section 5A. This explanation will subvert the need to justify the inclusion of property rights within the human rights practice.

In the following subsection, I will relate why data should be encompassed by property rights. This analysis will first provide a definition of property and explain how data may be accounted for by this definition. To justify the application of property rights to data, I will refer to Section 2 and discuss whether defining data as property can appropriately mitigate the harms from surveillance capitalism. I will also outline other extraneous benefits of classifying data as property. In the succeeding section, I will respond to relevant objections.

#### *Section 5A: The Pre-Existing Right to Property in the Human Rights Corpus*

The right to property is already enshrined in the human rights corpus. To provide some historical context, the 1648 Peace of Westphalia treaties created the modern state-system and

largely ended any conception of a global regime of property law.<sup>120</sup> Under this model, property rights were to be governed nationally through the domestic laws of particular states. This model contrasted with prevailing “natural law” theory, expounded by continental European scholars such as Grotius and Pufendorf, that emphasized the “universal right” of “private ownership.”<sup>121</sup> Under natural law theory, the state was created to protect pre-existing property rights. Within the common law system, John Locke was the foremost champion of the natural law approach to property.

Eventually, in 1765, William Blackstone would write the *Commentaries on the laws of England* which identified the right to property as one of three “absolute” rights in English law.<sup>122</sup> Domestically, Natural Law theory became increasingly popular in America and France during the late eighteenth century, and was wielded as a political tool during their respective revolutions.<sup>123</sup> However, it wasn’t until the mid-20th century and the formation of the Universal Declaration of Human Rights that the discourse around property rights shifted.<sup>124</sup>

Following the atrocities committed by Nazi Germany during the second world war, nations sought to establish international norms to clearly define the relationship between states and their nationals.<sup>125</sup> These norms were expressed as inalienable, fundamental, “human rights” that would be inviolable by all member parties. While there is a discernible connection between

---

<sup>120</sup> John G Sprankling, “Origins of International Property Law,” in *The International Law of Property* (Oxford: Oxford University Press, 2014), <https://doi.org/10.1093/acprof:oso/9780199654543.003.0001>.

<sup>121</sup> Stephen Buckle, “Hugo Grotius,” in *Natural Law and the Theory of Property* (Oxford: Oxford University Press, 1993), <https://doi.org/10.1093/acprof:oso/9780198240945.003.0001>.

<sup>122</sup> William Blackstone, “Book I: Of the Rights of Persons: Chapter I,” in *Commentaries on the Laws of England*, vol. 1 (New York: William E. Dean, 1853), i–ii, <https://heinonline.org/HOL/P?h=hein.beal/cmlengl0001&i=1>.

<sup>123</sup> Sprankling, “Origins of International Property Law.”

<sup>124</sup> See above.

<sup>125</sup> Johannes Morsink, “World War Two and the Universal Declaration,” *Human Rights Quarterly* 15, no. 2 (1993): 357–405, <https://doi.org/10.2307/762543>.

the intent behind the creation of human rights and the natural law tradition, academic debate as to the exact philosophical nature of human rights persists.<sup>126</sup>

Regardless of the exact philosophical background for the Universal Declaration of Human Rights, the right to property was first placed in Article 17 of the UDHR:

1. Everyone has the right to own property alone as well as in association with others.
2. No one shall be arbitrarily deprived of his property.<sup>127</sup>

Article 17 was groundbreaking in that it moved property away from the state's purview and vested it directly in the individual. Under this model, private citizens could assert property against their own state. However, due to dissension from the Soviet Bloc and other nations, this article was rejected, and a diluted version was instituted instead.<sup>128</sup>

1. The states parties to this Covenant undertake to respect the right of everyone to own property alone as well as in association with others. This right shall be subject to such limitations and restrictions as are imposed by law in the public interest and in the interest of social progress in the country concerned.
2. No one shall be deprived of his property without due process of law. Expropriation may take place only for considerations of public necessity or utility as defined by law and subject to such compensation as may be prescribed.<sup>129</sup>

Nevertheless, over the last 40 years, property law has become irrevocably encoded in the body of regional human rights law. Article 1 of the European Convention on Human Rights

---

<sup>126</sup> Cruft, Liao, and Renzo, *Philosophical Foundations of Human Rights*, 2.

<sup>127</sup> "Universal Declaration of Human Rights."

<sup>128</sup> Sprankling, "Origins of International Property Law."

<sup>129</sup> Theo R. G. van Banning, *The Human Right to Property* (Cambridge: Intersentia, 2002), [https://books.google.com/books/about/The\\_Human\\_Right\\_to\\_Property.html?id=X1EobCBveNUC](https://books.google.com/books/about/The_Human_Right_to_Property.html?id=X1EobCBveNUC).

(ECHR) states that “everyone has the right to the use and enjoyment of his property” and furthermore that “no one shall be deprived of his property except upon payment of just compensation...”<sup>130</sup> The ECHR is currently in force in 47 states, including the Russian Federation and other former Socialist states in Eastern Europe that rejected Article 17 in the original draft of the UDHR.<sup>131</sup>

Further examples include the African Charter on Human and Peoples Rights (ACHPR), which claims that “the right to property shall be guaranteed” and “may only be encroached upon in the interest of public need or in the general interest of the community.”<sup>132</sup> Article 21 of American Convention of Human Rights (ACHR) notes that “everyone has the right to the use and enjoyment of his property.”<sup>133</sup> These three conventions have enforcement power through established tribunals that are capable of hearing individual complaints.

In the Middle East and Asia, there are similar proclamations of the human right to property: Article 31 of the Arab Charter mentions that “everyone has a guaranteed right to own private property.”<sup>134</sup> The ASEAN Human Rights Declaration affirms that “every person has the right to own, use, dispose of and give that person’s lawfully acquired possessions alone or in association with others.”<sup>135</sup> While the Arab Charter and ASEAN Declaration are nonbinding legal instruments, their declaration of property as a human right wields normative power.<sup>136</sup>

---

<sup>130</sup> “European Convention on Human Rights,” *European Court of Human Rights*, n.d., 33.

<sup>131</sup> “47 Member States,” Council of Europe, accessed November 20, 2021, <https://www.coe.int/en/web/portal/47-members-states>.

<sup>132</sup> “African Charter on Human and Peoples’ Rights,” African Commission on Human and Peoples’ Rights, accessed November 24, 2021, <https://www.achpr.org/legalinstruments/detail?id=49>.

<sup>133</sup> “American Convention on Human Rights,” Inter-American Commission on Human Rights, accessed November 21, 2021, <https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm>.

<sup>134</sup> UN Office of the High Commissioner for Human Rights and League of Arab States, “Arab Charter on Human Rights,” 2004, 11, <https://digitallibrary.un.org/record/551368>.

<sup>135</sup> “ASEAN Human Rights Declaration,” Association of Southeast Asian Nations, November 19, 2012, <https://asean.org/asean-human-rights-declaration/>.

<sup>136</sup> Beth Simmons, *Mobilizing Human Rights: International Law in Domestic Politics* (Cambridge: Cambridge University Press, 2009).

In summary, a total of 132 states (over two-thirds of the entire UN membership) are party to binding human rights conventions that explicitly recognize the right to property.<sup>137</sup> Importantly, while human rights hold a peremptory position among international law norms, there are still a substantial number of countries (including China, India, and the United States) that are not part of human rights conventions recognizing the right to property.<sup>138</sup> Nevertheless, the right to property is encoded within a large subset of human rights laws and regulations.

### *Section 5B: Defining Property*

The key premise, and perhaps the most challenging one, is establishing that right to data should be conceived of in terms of property. The first difficulty is finding a concrete definition of property with transnational/cross-cultural applications. Modern conceptions of property rarely adhere to the traditional, Blackstonian concept of the “sole and despotic dominion in which one man claims and exercises over the external things of the world.”<sup>139</sup> The more common definition, influenced by Wesley Newcomb Hohfeld and Anthony Maurice Honoré, addresses property as a “bundle of rights” as prescribed by the state.<sup>140</sup> However, these theories largely pertain to a discussion of property in Anglo-American law and therefore cannot be generalized to the international sphere. In analyzing the possibility of introducing property rights to data in the EU, Ivan Stepanov uses David Lametti’s definition of property.<sup>141</sup>

---

<sup>137</sup> John G Sprankling, “Toward the Global Right to Property,” in *The International Law of Property* (Oxford: Oxford University Press, 2014), <https://doi.org/10.1093/acprof:oso/9780199654543.003.0009>.

<sup>138</sup> Andrea Bianchi, “Human Rights and the Magic of Jus Cogens,” *European Journal of International Law* 19, no. 3 (June 1, 2008): 491–508, <https://doi.org/10.1093/ejil/chn026>; Sprankling, “Toward the Global Right to Property.”

<sup>139</sup> Carol M. Rose, “Canons of Property Talk, or, Blackstone’s Anxiety,” *The Yale Law Journal* 108, no. 3 (1998): 601, <https://doi.org/10.2307/797498>.

<sup>140</sup> Denise R Johnson, “Reflections on the Bundle of Rights,” *Vermont Law Review* 32 (January 2007): 26.

<sup>141</sup> Ivan Stepanov, “Introducing a Property Right over Data in the EU: The Data Producer’s Right – an Evaluation,” *International Review of Law, Computers & Technology* 34, no. 1 (January 2, 2020): 65–86, <https://doi.org/10.1080/13600869.2019.1631621>.

“Private property is a social institution that comprises a variety of contextual relationships among individuals through objects of social wealth and is meant to serve a variety of individual and collective purposes. It is characterized by allocating to individuals a measure of control over the use and alienation of, some degree of exclusivity in the enjoyment of, and some measure of obligation to and responsibilities for scarce and separable objects of social wealth.”<sup>142</sup>

Similar to Stepanov, I will refer to Lametti’s view of property because it accounts for several arguments made in this thesis. For one, it accounts for property serving both “individual and collective” purposes, somewhat reconciling cross-cultural and ideological differences in the perception of property as serving individual or communal goals. This view also implies that property is a *relation to resources*, which better captures the language of data and surveillance capitalism; after all, the logic of surveillance capitalism involves mining digital exhaust – a resource generated by users –to synthesize behavioral predictions and eventually move towards behavioral automation.

### *Section 5C: Defining Data as Property*

First, it is relevant to establish that data is a resource. The American Heritage Dictionary provides two definitions of resource: “an available supply that can be drawn upon when needed” and “a means that can be used to advantage.”<sup>143</sup> My earlier discussion referred to the data used by surveillance capitalists as “digital exhaust” “behavioral surplus” or “collateral data.” These terms fit the general descriptions of a resource. For one, this data is constantly being generated

---

<sup>142</sup> David Lametti, “The Concept of Property: Relations Through Objects of Social Wealth,” *University of Toronto Law Journal* 53 (2003): 325–78.

<sup>143</sup> Anany V. Levitin and Thomas C. Redman, “Data as a Resource: Properties, Implications, and Prescriptions,” *Sloan Management Review* 40, no. 1 (Fall 1998): 91.



by users and fed into machine intelligence processes by corporations – ensuring an “available supply” –and the subsequently generated prediction products engender millions in profits for corporations, giving them a tangible advantage. If property is a relation to resources, then an individual’s relation to data can be understood as their right over this resource. To better illustrate this, I will provide an example that clarifies between a user’s interaction with the internet and the data that this interaction generates.

Till now, I have detailed how surveillance capitalism takes place through search engines, social media and other websites. However, this logic can also function through other computerized forms of technology that connect to the “cloud” – a form of storage that exists on the internet instead of a hard drive. In recent years, the promulgation of “wearables” – computerized clothing or accessories – has allowed sensitive consumer information to be transmitted to third parties and sold for profit.

A 2014 study by the FTC (Federal Trade Commission) found that twelve different health and fitness apps transmitted user data to 76 different third parties, including advertisers.<sup>144</sup> In short, the manifestations of the user’s human experiences, like their heartbeat, sleep patterns and exercise routines, can be digitized and commodified. A user’s heartbeat in and of itself does not constitute their “property,” however, when it is translated into data, it invariably becomes a resource and thus an “object of social wealth.” From this vantage point, property rights to data are generated through the translation of human experiences into data. While I use this example to more clearly distinguish between the human experience itself (which does not constitute property) and the rendition of this experience into data – the same principle applies to all forms of online behavior.

---

<sup>144</sup> Matthew R. Langley, “Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables,” *Georgetown Law Journal* 103, no. 6 (2015 2014): 1641–60.

*Section 5D: Examining How the Property Right to Data can Address Surveillance Capitalism's Harms*

Could establishing property rights to data sufficiently address the harms perpetuated by surveillance capitalism? As a reminder, surveillance capitalism threatens values of autonomy, freedom, and distributive justice (see Section 2). With respect to autonomy, property rights would transfer some measure of control over an individual's data back to the user themselves. Conceiving of the “means to an end” argument as a flow that situates users as “means” and firms' profits from data-driven analytics as the “end” yields a better understanding of this claim – users are given a stake in the transition between raw data exhaust and predictive product. The creation of an “interventionary stage” allows users far more autonomy because it grants them some agency in what occurs to their data rather than rendering them passive generators of profits for corporations.

This might sound like a speculative claim, however, there is evidence in behavioral economics that suggests that people imbue objects that they *own* with higher value relative to if they don't own these objects. Richard Thaler referred to this pattern as the “endowment effect,” which he describes as “the fact that people often demand much more to give up an object they are endowed with than they would be willing to pay to acquire it.”<sup>145</sup> In 1990, Daniel Kahneman and his colleagues tested this theory, organizing a market for mugs in which half the subjects were randomly chosen to be endowed with a mug, and the other half were not endowed with a

---

<sup>145</sup> Daniel Kahneman, Jack L. Knetsch, and Richard H. Thaler, “Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias,” *Journal of Economic Perspectives* 5, no. 1 (March 1991): 194, <https://doi.org/10.1257/jep.5.1.193>.

mug.<sup>146</sup> Those not endowed with a mug were asked to list their selling price, while those with a mug were asked to list their buying price.

If preferences were unaffected by the creation of property rights, then selling prices should be equal to buying prices, and around half the mugs should be traded. Instead, Kahneman found that the number of trades were lower than expected: sellers demanded more for the mugs they owned than buyers were willing to pay.<sup>147</sup> This study suggests that granting an individual property rights to an object intensifies the attachment they feel to said object. In the realm of data, this suggests that the creation of property rights will heighten the attachment an individual experiences to their data.

With regards to autonomy, rather than seeking to presume the will of the individual, property rights essentially force an individual to consider *what* their will is by augmenting the emotional attachment an individual feels to their data. If users own their data exhaust, they be more likely to critically evaluate what they want to happen to it. This also prevents the subversive manipulation of an individual's will "without consent," since they are explicitly forced to consider what their personal will may be at an early stage in the process.

Finally, the endowment theory is considered to be a product of "loss aversion"—a theory that describes how individuals experience more disutility from *losing* an object relative to the utility they experience when they acquire an object.<sup>148</sup> I argue that the phenomenon of loss aversion as it relates to endowment theory will prevent users from trading away their property rights the same way they sign away their privacy rights. Granting ownership over an object

---

<sup>146</sup> Daniel Kahneman, Jack L. Knetsch, and Richard H. Thaler, "Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias," *Journal of Economic Perspectives* 5, no. 1 (March 1991): 193–206, <https://doi.org/10.1257/jep.5.1.193>.

<sup>147</sup> Kahneman, Knetsch, and Thaler, "Experimental Tests of the Endowment Effect and the Coase Theorem."

<sup>148</sup> Kahneman, Knetsch, and Thaler, "Experimental Tests of the Endowment Effect and the Coase Theorem."

essentially heightens the effects of loss aversion; as such, I postulate that individuals will more experience more disutility from losing data when they explicitly own it.

Of course, one might argue that privacy protections and the opt-out function also grant users autonomy by forcing them to consider their personal will. There are two responses to this objection: first, that empirical evidence already demonstrates that users typically pay little heed to the privacy contracts offered to them when accessing a website. Nonetheless, this is a behavioral quirk of humans, one that could easily be circumvented by, for instance, offering opt-out as the default choice. Under this model, individuals would have to actively choose to opt-in rather than the opposite. This would entail a “paternalistic” approach – a mechanism by which an actor’s actions are limited or prohibited on the grounds that it “would be contrary to the actor’s own welfare.”<sup>149</sup>

Behavioral research proves that this mechanism could be highly effective; a study by Eric J. Johnson and Steven Bellman found that when asking participants whether they would like to be contacted for future surveys, framing the question as “opting out” resulted in 96.3% of participants agreeing, while only 48.2% agreed to be contacted when the question was framed as “opting in.”<sup>150</sup> The concern here is that a paternalistic approach also limits individual autonomy. Since this mechanism of redress causes the same form of harm as the issue of surveillance capitalism itself, default opt-out privacy contracts are less appealing than property frameworks in this domain. With the property framework, the authority remains squarely with the individual, offering more autonomy.

---

<sup>149</sup> Anthony T. Kronman, “Paternalism and the Law of Contracts,” *The Yale Law Journal* 92, no. 5 (April 1983): 763, <https://doi.org/10.2307/796144>.

<sup>150</sup> Eric J. Johnson, Steven Bellman, and Gerald L. Lohse, “Defaults, Framing and Privacy: Why Opting In-Opting Out1,” *Marketing Letters* 13, no. 1 (February 1, 2002): 5–15, <https://doi.org/10.1023/A:1015044207315>.

In Section 2B, I also discussed a broader model of autonomy which focused on the two stages of self-determination and related to self-censorship. Regarding the process of self-determination, users could still choose to sign away their property rights and still be on the receiving end of harmful marketing practices. I contend that any regime actively preventing selective marketing would have to be intrinsically paternalistic, as it would have to take the choice for data exhaust being processed out of the user's hands altogether.

There would certainly have to be other measures or legislation in place to prevent the negative effects of selective marketing. However, a property rights framework could incentivize people to ask the right questions and result in individuals more critically evaluating the effects of signing away something that they own. This could stem from the endowment effects and loss aversion; people might be less likely to sign away their rights to their data given the intensified emotional attachment over objects that they own.

A possible concern here is that data, unlike the objects described in the aforementioned studies, is a tangible object: would the loss aversion and endowment effect still apply to intangibles? While there is no research detailing the impact of loss aversion or the endowment effect on data, there is research studying these phenomena on another type of intangible property: intellectual property rights. In a 2010 study, Christopher J. Buccafusco studied the effect of assigning property rights over intellectual property amongst 3 groups: creators, owners, and buyers.<sup>151</sup> The creators were asked to write a haiku for a poetry competition, and then asked to list the lowest price they would accept for the poem. The buyers were each shown one poem

---

<sup>151</sup> Christopher J. Buccafusco and Christopher Jon Sprigman, "Valuing Intellectual Property: An Experiment," *SSRN Electronic Journal*, 2010, <https://doi.org/10.2139/ssrn.1568962>.

and asked to list the highest price they were willing to pay. Finally, the owners were assigned the intellectual property rights the poems, and also asked to list their lowest asking price.

Buccafusco found that that there was no statistically significant gap between the prices listed by the owners or the creators, however, there was a significant divide between these prices and the amount the buyers were willing to pay.<sup>152</sup> This indicates that the owners, by mere possession of the property right, valued the intangible object more than the buyers (who did not possess property rights) did. Therefore, we have good reason to think that even though data is an intangible object, establishing a property rights regime could inspire similar behavioral effects.

Regarding the second aspect of autonomy (decision-making), property rights could remediate the possibility of self-censorship because it acts as an assurance that users have a concrete claim to their data. Psychologically, it could alleviate concerns that their data is being surreptitiously collected. Instead, users may feel that they have active agency over their data when interacting with the internet. This is a somewhat conjectural claim, however there is some generalized theoretical evidence to support this notion.

In a 1998 study, E. Kevin Kelloway, Julian Barling, and Anthony E. Carroll found that property rights to jobs resulted in positive correlates of perception relevant to an employment stimulus, such as increased organizational commitment, increased perceptions of control, and organizational tenure.<sup>153</sup> Specifically, property rights to job was associated with a sense of *job security* or control over the job. Extrapolating these results to data, we can presume that granting individuals property rights of data will increase their perception of control over the data, and possibly even impart a feeling of data security.

---

<sup>152</sup> Buccafusco and Sprigman, "Valuing Intellectual Property."

<sup>153</sup> E. Kevin Kelloway, Julian Barling, and Anthony E. Carroll, "Perceived Causes and Consequences of Property Rights to Jobs," *Journal of Business and Psychology* 12, no. 4 (1998): 505–13.

Turning to the second harm associated with surveillance capitalism, could property rights effectively remediate the limitations placed on capabilities? As I discussed earlier, the creation of property rights will not necessarily eradicate selective marketing. Similarly, it will not eliminate the use of “alternative data,” in inhibiting self-determination, nor can it extinguish the creation of algorithm “filter-bubbles” and the narrowing of the online world altogether. Users will always have the choice to allow these phenomena to occur by choosing to forfeit their data. Since property rights may not sufficiently address the harms of surveillance capitalism to capabilities, there is grounds for a valid objection here.

In response, I refer to the previous discussion of endowment effect and loss aversion, to hypothesize that a property rights framework could generate more incentive to critically consider the relinquishment of one’s data. Implying that a person *owns* their data creates a normative power of possessiveness that may instigate individuals to critically evaluate whether they want to give up their data. Given the lacunae in research on property rights over data however, this is still a speculative claim.

Another theory of human behavior that might validate the argument for data as property is the “mere ownership effect” proposed by Fritz Heider. Heider proposes that since possessions are objects associated with the self, perceiving them and making judgments about them is a social process susceptible to the same self-enhancing biases that affect individual’s perceptions of themselves.<sup>154</sup> This theory was tested by James Beggan in 1992, who found that “people overvalue an object associated with the self, namely, an owned object.”<sup>155</sup> Therefore, given that individuals give more normative value to objects they own, this could encourage them to

---

<sup>154</sup> James K. Beggan, “On the Social Nature of Nonsocial Perception: The Mere Ownership Effect,” *Journal of Personality and Social Psychology* 62, no. 2 (1992): 230, <https://doi.org/10.1037/0022-3514.62.2.229>.

<sup>155</sup> James K. Beggan, “On the Social Nature of Nonsocial Perception: The Mere Ownership Effect,” 235.

contemplate relinquishing the rights to data that they own more than they would relative to if they did not have this ownership claim.

By extension, the property rights framework could encourage individuals to become more informed about the ramifications of renouncing their data; when the language of property comes into play, people may be more likely to take the time to research and puzzle out their options rather than acting on more impulsive whims (as is the case with the opt-in/opt-out option for privacy). Ultimately, this will be contingent on how the property rights framework takes shape, and whether it will attach a monetary value to personal data. This is a point I will discuss further in the next paragraph.

The third harm discussed in Section 2C of this paper details the threats of surveillance capitalism to distributive justice and equality of opportunity. Once again, the extent to which a property rights framework could adequately address this concern is dependent on what form it takes: if monetary compensations are attached to personal data exhaust, then there is a possibility that the property rights framework could worsen the inequalities perpetuated by surveillance capitalism. If the property rights framework allows people exchange their data for money, then it is likely that already disadvantaged individuals will make this choice. For example, individuals with low credit scores or in financial stress may be more likely to sell their data, which would allow surveillance capitalist tactics to further discriminate against them when they are searching for employment or housing.

Perhaps, however, there is an alternative way to look at this issue. Jaron Lanier and E. Glen Weyl propose a society of “data dignity” – where people will be paid for their data and will pay for services that require data from others.<sup>156</sup> In their envisioned proposal, individuals’

---

<sup>156</sup> Jaron Lanier and E Glen Weyl, “A Blueprint for a Better Digital Society,” *Harvard Business Review*, September 2018, 4.



attention will be guided by their self-defined interests rather than manipulative, targeted platform. Correspondingly, platforms will receive higher quality data to train their machine learning systems. Lanier and Weyl hypothesize that the creation of “Mediators of Individual Data” or MIDS can mediate this market. A MID functions as a sort of union, consisting of a group of volunteers that represents its online members in a wide range of ways – including the negotiation of data royalties.<sup>157</sup> If property rights were to be attached to financial incentives, MIDs could offset some of the potential issues to do with distributive justice concerns through collective bargaining. The class of “those who have data” will be afforded more concentrated power through the creation of groups dedicated to promoting their interests.

Of course, it is not necessary that property rights take the shape of data dignity at the human rights level. However, property rights offer the necessary background to create more specific legislation, either at the domestic or international level, that could advance the concept of personal data with *value*. This is largely because property rights, in line with the definition I offered, conceptualizes data as a resource. Nevertheless, a detailed account of how data as property could take effect at different levels is beyond the scope of this paper: I merely offer this proposal as an example of how property rights *could* theoretically remediate a specific harm associated with surveillance capitalism.

One worry that might arise here could be the feasibility of an international property system at present. I agree that institutionalizing an international property scheme for data, especially one that would allow people to press claims, might be unrealistic at present. But, data could be encoded as property at the international human rights level, which would not require establishing an international property system. This classification may inspire normative changes:

---

<sup>157</sup> Lanier and Weyl, “A Blueprint for a Better Digital Society,” 5.

previous research by Beth Simmons has demonstrated that human rights contain extensive normative power by entrapping countries into “toeing” a line.<sup>158</sup>

Lastly, there is a more general motivation for classifying data as property. Indisputably, most Western legal systems are fiercely protective of private property. Though there may be regional variations in *how* property is defined, Western legal systems “give great emphasis to the concept of possession.”<sup>159</sup> In *Capital and Ideology*, Thomas Piketty argues that all political and property regimes have remained inextricably intertwined in *all* societal and cultural structures: from communist and social-democratic societies to modern postcolonial and hyper capitalist communities.<sup>160</sup> There are usually penalties circumscribed in existing legal systems to address property breaches.

Therefore, there is good reason to think that personal property entitlements to data will generate claims that are difficult for corporations to dismiss. With respect to cross-cultural validity, the concept of communal or shared property is more common in Non-Western legal traditions. As Piketty notes, however, property rights are still “persistently linked” to the organization of a political regime.<sup>161</sup> Given that most societies give property claims a great deal of weight, it is reasonable to conclude that property entitlements to data will instigate transnational claims that are difficult to ignore.

Moreover, the designation of data as property at the human rights level could give rise to more regional legislation on data protection. Simmons discusses how human rights treaties specifically can change the national policy agenda and enhance the possibility of litigation at the

---

<sup>158</sup> Simmons, *Mobilizing Human Rights: International Law in Domestic Politics*.

<sup>159</sup> The Editors of Encyclopaedia Britannica, “Property,” in *Encyclopedia Britannica*, February 12, 2021, <https://www.britannica.com/topic/property-legal-concept>.

<sup>160</sup> Thomas Piketty, *Capital and Ideology*, (Cambridge: Harvard University Press, 2020), <https://doi.org/10.4159/9780674245075>.

<sup>161</sup> Piketty, *Capital and Ideology*

supranational level.<sup>162</sup> Perhaps the designation of data as property at the human rights level would create change at a regional scale, bolstering domestic laws to provide even more protection for internet users. We can imagine that the designation of data as property at the international scale would give rise to more national legislation, leading to a stronger network of rules and regulations that protect users from the threats of surveillance capitalism.

## **Section 6: Objections to the Argument for Data as Property**

I will now consider objections specific to classifying data as property. First, one might be unpersuaded by the claim that classifying data as property is the best way to protect individuals from the harms discussed in Section 2. Such a skeptic may argue that the best way to protect users from the threats posed by surveillance capitalism is to ban the rendition of human experience into data or to stop the generation of this data exhaust in the first place. Essentially, there must be practices in place that prevent corporations from rendering users' interactions with the internet into profitable data points.

This type of detractor would argue that property is the incorrect approach because the property argument accepts that this data exhaust has been generated in the first place, while an alternative approach would not cede this point. A skeptic with this view might tout privacy laws as the best mechanism of achieving this. In response, I claim that this approach may remediate the harms to distributive justice arising from surveillance capitalism but remains paternalistic in assuming that users don't want their experiences rendered into data to begin with. Like the argument I made in Section 5, assuming the will of any given user is a clear infringement of their autonomy.

---

<sup>162</sup> Simmons, *Mobilizing Human Rights*.

Furthermore, as I briefly outlined in Section 2, the generation of digital exhaust does yield some benefits, like personalized content and consumer satisfaction. With respect to targeted advertising specifically, corporations have generated profits that are beneficial to economies. It is my view that a property framework, rather than a terminal ban on the generation of this data altogether, would allow for these benefits to be generated within the constraints imposed by the values of autonomy, freedom, and distributive justice.

There is also the possibility of a property rights framework, like the one proposed by Lanier and Weyl, that specifically addresses the issues to do with autonomy, freedom and distributive justice while still allowing for the generation of economic benefits (see section 5D). For these reasons, I consider defining data in terms of property to be a more nuanced response. The view of data as property is responsive to the harms from surveillance capitalism, while allowing potential economic benefits from selective marketing practices to thrive.

There may be critics who remain unconvinced by the property approach because of the normative implications that accompany declaring data property. For instance, though I have addressed the transnational recognition of private property through Piketty's view, a skeptic might remain unconvinced and assert that private property is not a universally recognized value. This critique might argue that the concept of private property will not hold weight in collectivist societies. A related criticism is that if property rights do necessitate the creation of an entirely new market for the buying and selling of personal data, there may be unwanted economic repercussions. In response to this broad class of objections that object to the universality of property or the manifestations of a property framework, I propose that property rights need not exist in a vacuum.

Property rights could simply be another tool at the human rights level wielded to mitigate the harms of surveillance capitalism. My earlier discussion of the limitations of existing privacy laws becomes relevant here: as previously argued, the current regime, as it exists, is not robust enough. This paper develops an argument for a novel solution that could address the previously stated harms of surveillance capitalism, but perhaps this solution is to be used in *conjunction* with bolstered privacy laws to completely eradicate the harms. Essentially, by arguing for the limitations of current privacy law or potential privacy laws, I do not mean to undermine the efficacy of privacy in the data sphere altogether. Instead, I hope to open an alternative avenue that could address some of the lacunae present in existing legislative measures.

## **Conclusion**

Ultimately, any solution to the issue of surveillance capitalism will require a mechanism that forces us to reconsider and realize the true value of personal data. As such, the solution might lie in an institution that humans have held in high regard for centuries. The inclusion of property rights in conjunction with any other effective approach could address the problem from a variety of perspectives, while ensuring a certain element of practicality. It may be unrealistic to expect to eliminate surveillance capitalism altogether, however, we can redirect this logic of economic accumulation by capitalizing off individuals to an end that better serves both the user and the corporations.

In this research, I detailed how the right to individual data is pre-existing in the human rights corpus, using the political conception of human rights to argue that the right to data fits the general criteria for what should constitute a human right. While my analysis was largely restricted to the works of Rawls, Beitz and Raz, further scholarship could strive for a more

generalized account of the right to data as a human right under this lens. Additionally, there is potential for research into this argument from an orthodox or naturalistic perspective; this could serve to convince detractors of the political conception by conceptualizing the right to data as an intrinsically moral right.

My argument for why data should constitute property largely relied on my analysis of the harms stemming from surveillance capitalism, namely, the threats to autonomy, freedom, and distributive justice. These are broad harms meant to apply cross-culturally, however, further insights into regional perceptions of the threats of surveillance capitalism could better inform supranational models of protection. Moreover, this intuition could lead to a more culturally attuned vision of data as property at the global scale. In arguing for why data should constitute property, I also discussed possible models for implementation. Lanier and Weyl's model is a good starting point, but future research should focus on amalgamating both privacy and property into a singular model to better account for the normative concerns to do with implementing property rights. As far as solutions to surveillance capitalism go, the discussion has only begun: progress will require interdisciplinary analysis that may originate from the philosophical domain, but must coalesce with insights from international relations, economics, law, and business.

## Bibliography

- African Commission on Human and Peoples' Rights. "African Charter on Human and Peoples' Rights." Accessed November 24, 2021. <https://www.achpr.org/legalinstruments/detail?id=49>.
- African Union. "African Union Convention on Cyber Security and Personal Data Protection," June 27, 2014. <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>
- Aitken, Rob. "'All Data Is Credit Data': Constituting the Unbanked." *Competition & Change* 21 (June 20, 2017). <https://doi.org/10.1177/1024529417712830>.
- Inter-American Commission on Human Rights. "American Convention on Human Rights." Accessed November 21, 2021. <https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm>.
- Armstrong, Chris. "Global Equality of Opportunity." In *Encyclopedia of Global Justice*, edited by Deen K. Chatterjee, 410–11. Dordrecht: Springer Netherlands, 2011. [https://doi.org/10.1007/978-1-4020-9160-5\\_277](https://doi.org/10.1007/978-1-4020-9160-5_277).
- Association of Southeast Asian Nations. "ASEAN Human Rights Declaration," November 19, 2012. <https://asean.org/asean-human-rights-declaration/>.
- "Avalon Project - Blackstone's Commentaries on the Laws of England - Book the First - Chapter the First : Of the Absolute Rights of Individuals." Accessed December 21, 2021. [https://avalon.law.yale.edu/18th\\_century/blackstone\\_bk1ch1.asp](https://avalon.law.yale.edu/18th_century/blackstone_bk1ch1.asp).
- Banisar, David, and Simon Davies. "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments." *UIC John Marshall Journal of Information Technology & Privacy Law* 18, no. 1 (January 1, 1999). <https://repository.law.uic.edu/jitpl/vol18/iss1/1>.
- Banning, Theo R. G. van. *The Human Right to Property*. Cambridge: Intersentia, 2002. [https://books.google.com/books/about/The\\_Human\\_Right\\_to\\_Property.html?id=X1EobCBveNUC](https://books.google.com/books/about/The_Human_Right_to_Property.html?id=X1EobCBveNUC).
- Beggan, James K. "On the Social Nature of Nonsocial Perception: The Mere Ownership Effect." *Journal of Personality and Social Psychology* 62, no. 2 (1992): 229–37. <https://doi.org/10.1037/0022-3514.62.2.229>.
- Beitz, Charles R. *The Idea of Human Rights*. Oxford: Oxford University Press, 2009. <https://doi.org/10.1093/acprof:oso/9780199572458.001.0001>.
- Bianchi, Andrea. "Human Rights and the Magic of Jus Cogens." *European Journal of International Law* 19, no. 3 (June 1, 2008): 491–508. <https://doi.org/10.1093/ejil/chn026>.
- Blackstone, William. "Book I: Of the Rights of Persons: Chapter I." In *Commentaries on the Laws of England*, 1:i–ii. New York: William E. Dean, 1853. <https://heinonline.org/HOL/P?h=hein.beal/cmlengl0001&i=1>.
- Bond, Robert M., Christopher J. Fariss, Jason J. Jones, Adam D. I. Kramer, Cameron Marlow, Jaime E. Settle, and James H. Fowler. "A 61-Million-Person Experiment in Social Influence and Political Mobilization." *Nature* 489, no. 7415 (September 2012): 295–98. <https://doi.org/10.1038/nature11421>.
- Britannica, The Editors of Encyclopaedia. "Property." In *Encyclopedia Britannica*, February 12, 2021. <https://www.britannica.com/topic/property-legal-concept>.
- Brock, Gillian. "Equality of Opportunity and Global Justice." In *The Oxford Handbook of Global Justice*, edited by Thom Brooks. Oxford: Oxford University Press, 2020. <https://doi.org/10.1093/oxfordhb/9780198714354.001.0001>.

- Buccafusco, Christopher J., and Christopher Jon Sprigman. “Valuing Intellectual Property: An Experiment.” *SSRN Electronic Journal*, 2010. <https://doi.org/10.2139/ssrn.1568962>.
- Buckle, Stephen. “Hugo Grotius.” In *Natural Law and the Theory of Property*. Oxford: Oxford University Press, 1993. <https://doi.org/10.1093/acprof:oso/9780198240945.003.0001>.
- Bussell, Jennifer. “Cyberspace.” In *Encyclopedia Britannica*, March 12, 2013. <https://www.britannica.com/topic/cyberspace>.
- Caney, Simon. *Justice Beyond Borders: A Global Political Theory*. Oxford: Oxford University Press, 2005. <https://doi.org/10.1093/019829350X.001.0001>.
- Carter, Ian. “Positive and Negative Liberty.” In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Winter 2021. Metaphysics Research Lab, Stanford University, 2021. <https://plato.stanford.edu/archives/win2021/entries/liberty-positive-negative/>.
- Chan, Joseph. “Moral Autonomy, Civil Liberties, and Confucianism.” *Philosophy East and West* 52, no. 3 (2002): 281–310.
- Chivers, Dean. “Personal Data Protection in Africa.” Deloitte, 2017. <https://www2.deloitte.com/za/en/pages/risk/articles/personal-data-protection-in-africa.html>.
- Cinnamon, Jonathan. “Social Injustice in Surveillance Capitalism.” *Surveillance & Society* 15, no. 5 (December 5, 2017): 609–25. <https://doi.org/10.24908/ss.v15i5.6433>.
- Clark, David. “The Capability Approach: Its Development, Critiques and Recent Advances.” *Global Poverty Research Group* 2 (January 1, 2005). [https://base.socioeco.org/docs/developments\\_critiques\\_advances.pdf](https://base.socioeco.org/docs/developments_critiques_advances.pdf).
- Council of Europe. “47 Member States.” Accessed December 21, 2021. <https://www.coe.int/en/web/portal/47-members-states>.
- Crawford, Kate, and Jason Schultz. “Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms.” *Boston College Law Review* 55, no. 1 (January 29, 2014): 93.
- Cruft, Rowan, Matthew Liao, and Massimo Renzo, eds. *Philosophical Foundations of Human Rights*. Philosophical Foundations of Law. Oxford: Oxford University Press, 2015. <https://doi.org/10.1093/acprof:oso/9780199688623.001.0001>.
- Darwall, Stephen. “The Value of Autonomy and Autonomy of the Will.” *Ethics* 116, no. 2 (January 1, 2006): 263–84. <https://doi.org/10.1086/498461>.
- “Data Protection Commissioner v. Facebook Ireland Ltd.” *Harvard Law Review* 134, no. 4 (February 21, 2021). <https://harvardlawreview.org/2021/02/data-protection-commissioner-v-facebook-ireland-ltd/>.
- Deibert, Ronald J., and Masashi Crete-Nishihata. “Global Governance and the Spread of Cyberspace Controls.” *Global Governance* 18, no. 3 (2012): 339–61.
- “DIGITAL FOOTPRINT (Noun).” In *Macmillan Dictionary*. Accessed December 8, 2021. <https://www.macmillandictionary.com/us/dictionary/american/digital-footprint>.
- “European Convention on Human Rights.” *European Court of Human Rights*, n.d., 34.
- Feldman, Noah. “Political Equality and the Islamic State.” *Philosophical Topics* 30, no. 2 (2002): 253–72.
- Foucault, Michel. “‘Panopticism’ from ‘Discipline & Punish: The Birth of the Prison.’” *Race/Ethnicity: Multidisciplinary Global Contexts* 2, no. 1 (2008): 1–12.
- GAO, Ruiquan, and Xin YAN. “The Source of the Idea of Equality in Confucian Thought.” *Frontiers of Philosophy in China* 5, no. 4 (2010): 486–505.
- Gerards, Janneke. “The Fundamental Rights Challenges of Algorithms.” *Netherlands Quarterly of Human Rights* 37, no. 3 (September 1, 2019): 205–9. <https://doi.org/10.1177/0924051919861773>.



- “Global Chilling: The Impact of Mass Surveillance on International Writers.” PEN American Center, January 5, 2015. <https://pen.org/research-resources/global-chilling/>.
- Goldman, David. “Google: The Reluctant Censor of the Internet.” *CNNMoney*, January 4, 2015. <https://money.cnn.com/2015/01/04/technology/google-censorship/index.html>.
- Google. “Google Economic Impact,” 2020. <https://economicimpact.google.com/introduction/>.
- Graaf, Francisca Christina Wilhelmina de. “Dworkin’s Constructive Interpretation as a Method of Legal Research.” *Law and Method*, no. 12 (2015). <https://doi.org/10.5553/REM/000012>.
- Grafanaki, Sofia. “Autonomy Challenges in the Age of Big Data.” *Fordham Intellectual Property, Media and Entertainment Law Journal* 27, no. 4 (May 15, 2017): 803.
- Hern, Alex. “Cambridge Analytica: How Did It Turn Clicks into Votes?” *The Guardian*, May 6, 2018, sec. News. <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>.
- Herschel, Richard, and Virginia M. Miori. “Ethics & Big Data.” *Technology in Society* 49 (May 2017): 31–36. <https://doi.org/10.1016/j.techsoc.2017.03.003>.
- Heyman, Steven. “Positive and Negative Liberty.” *Chicago-Kent Law Review* 68, no. 1 (December 1, 1992): 81.
- Jaurisch, Julian, and Aline Blankertz. “What the European DSA and DMA Proposals Mean for Online Platforms.” *Brookings* (blog), January 14, 2021. <https://www.brookings.edu/techstream/what-the-european-dsa-and-dma-proposals-mean-for-online-platforms/>.
- Johnson, Denise R. “Reflections on the Bundle of Rights.” *Vermont Law Review* 32 (January 2007): 26.
- Johnson, Eric J., Steven Bellman, and Gerald L. Lohse. “Defaults, Framing and Privacy: Why Opting In-Opting Out.” *Marketing Letters* 13, no. 1 (February 1, 2002): 5–15. <https://doi.org/10.1023/A:1015044207315>.
- Kahneman, Daniel, Jack L. Knetsch, and Richard H. Thaler. “Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias.” *Journal of Economic Perspectives* 5, no. 1 (March 1991): 193–206. <https://doi.org/10.1257/jep.5.1.193>.
- . “Experimental Tests of the Endowment Effect and the Coase Theorem.” *Journal of Political Economy* 98, no. 6 (1990): 1325–48.
- Kelloway, E. Kevin, Julian Barling, and Anthony E. Carroll. “Perceived Causes and Consequences of Property Rights to Jobs.” *Journal of Business and Psychology* 12, no. 4 (1998): 505–13.
- Kleist, Chad. “Global Ethics: Capabilities Approach.” In *Internet Encyclopedia of Philosophy*. Accessed April 18, 2022. <https://iep.utm.edu/ge-capab/>.
- Kozyreva, Anastasia, Philipp Lorenz-Spreen, Ralph Hertwig, Stephan Lewandowsky, and Stefan M. Herzog. “Public Attitudes towards Algorithmic Personalization and Use of Personal Data Online: Evidence from Germany, Great Britain, and the United States.” *Humanities and Social Sciences Communications* 8, no. 1 (May 14, 2021): 1–11. <https://doi.org/10.1057/s41599-021-00787-w>.
- Kronman, Anthony T. “Paternalism and the Law of Contracts.” *The Yale Law Journal* 92, no. 5 (April 1983): 763–98. <https://doi.org/10.2307/796144>.
- Laidler, John. “Harvard Professor Says Surveillance Capitalism Is Undermining Democracy.” *Harvard Gazette* (blog), March 4, 2019. <https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/>.
- Lametti, David. “The Concept of Property: Relations Through Objects of Social Wealth.” *University of Toronto Law Journal* 53 (2003): 325–78.

- Lamont, Julian, and Christi Favor. "Distributive Justice." In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Winter 2017. Metaphysics Research Lab, Stanford University, 2017. <https://plato.stanford.edu/archives/win2017/entries/justice-distributive/>.
- Langley, Matthew R. "Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables." *Georgetown Law Journal* 103, no. 6 (2015 2014): 1641–60.
- Langvatn, Silje A. "Legitimate, but Unjust; Just, but Illegitimate: Rawls on Political Legitimacy." *Philosophy & Social Criticism* 42, no. 2 (February 2016): 132–53. <https://doi.org/10.1177/0191453715615386>.
- Lanier, Jaron, and E Glen Weyl. "A Blueprint for a Better Digital Society." *Harvard Business Review*, September 2018, 18.
- Leiner, Barry M, Robert E Kahn, and Jon Postel. "A Brief History of the Internet." *ACM SIGCOMM Computer Communication Review* 39, no. 5 (2009): 10.
- Levey, Geoffrey Brahm. "Equality, Autonomy, and Cultural Rights." *Political Theory* 25, no. 2 (1997): 215–48.
- Levin, Sam. "Facebook Told Advertisers It Can Identify Teens Feeling 'insecure' and 'Worthless.'" *The Guardian*, May 1, 2017, sec. Technology. <https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens>.
- Levitin, Anany V., and Thomas C. Redman. "Data as a Resource: Properties, Implications, and Prescriptions." *Sloan Management Review* 40, no. 1 (Fall 1998): 89–101.
- Lindecrantz, Erik, Madeleine Tjon Pian Gi, and Stefano Zerbi. "Personalized Experience for Customers: Driving Differentiation in Retail | McKinsey." *McKinsey & Company*, April 28, 2020. <https://www.mckinsey.com/industries/retail/our-insights/personalizing-the-customer-experience-driving-differentiation-in-retail>.
- Long, Ryan. "Egalitarianism." In *Internet Encyclopedia of Philosophy*. Accessed December 20, 2021. <https://iep.utm.edu/egalitar/>.
- Manovich, Lev. "Trending: The Promises and the Challenges of Big Social Data." In *Debates in the Digital Humanities*. University of Minnesota Press, 2012. <https://doi.org/10.5749/minnesota/9780816677948.003.0047>.
- Martins, Nuno. "Realism, Universalism and Capabilities." *Review of Social Economy* 65, no. 3 (2007): 253–78.
- Mayer-Schönberger, Viktor, and Kenneth Cukier. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston: Houghton Mifflin Harcourt, 2013.
- Miller, David. "Justice." In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Fall 2021. Metaphysics Research Lab, Stanford University, 2021. <https://plato.stanford.edu/archives/fall2021/entries/justice/>.
- Morsink, Johannes. "World War Two and the Universal Declaration." *Human Rights Quarterly* 15, no. 2 (1993): 357–405. <https://doi.org/10.2307/762543>.
- Naughton, John. "The Evolution of the Internet: From Military Experiment to General Purpose Technology." *Journal of Cyber Policy* 1, no. 1 (January 2, 2016): 5–28. <https://doi.org/10.1080/23738871.2016.1157619>.
- Obar, Jonathan, and Anne Oeldorf-Hirsch. "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services." *Information, Communication & Society* 23 (July 3, 2018): 1–20. <https://doi.org/10.1080/1369118X.2018.1486870>.

- Piketty, Thomas. *Capital and Ideology*. *Capital and Ideology*. Cambridge: Harvard University Press, 2020. <https://doi.org/10.4159/9780674245075>.
- Eur-Lex. “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Contestable and Fair Markets in the Digital Sector (Digital Markets Act).” European Union Law. Accessed December 22, 2021. <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN>.
- Rainie, Lee and Anderson, Janna. “The Fate of Online Trust in the Next Decade.” *Pew Research Center* (blog), August 10, 2017. <https://www.pewresearch.org/internet/2017/08/10/the-fate-of-online-trust-in-the-next-decade/>.
- Rawls, John. “The Law of Peoples.” *Critical Inquiry* 20, no. 1 (1993): 36–68.  
———. *The Law of Peoples: With “The Idea of Public Reason Revisited.”* Cambridge: Harvard University Press, 2001. <https://doi.org/10.2307/j.ctv1pncngc>.
- Raz, Joseph. “Human Rights Without Foundations.” *Oxford Legal Studies Research*, January 1, 2007. [https://scholarship.law.columbia.edu/faculty\\_scholarship/1491](https://scholarship.law.columbia.edu/faculty_scholarship/1491).
- Robeyns, Ingrid, and Morten Fibieger Byskov. “The Capability Approach.” In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Winter 2021. Metaphysics Research Lab, Stanford University, 2021. <https://plato.stanford.edu/archives/win2021/entries/capability-approach/>.
- Rose, Carol M. “Canons of Property Talk, or, Blackstone’s Anxiety.” *The Yale Law Journal* 108, no. 3 (1998): 601–32. <https://doi.org/10.2307/797498>.
- Sætra, Henrik Skaug. “The Tyranny of Perceived Opinion: Freedom and Information in the Era of Big Data.” *Technology in Society* 59 (November 1, 2019). <https://doi.org/10.1016/j.techsoc.2019.101155>.  
———. “When Nudge Comes to Shove: Liberty and Nudging in the Era of Big Data.” *Technology in Society* 59 (November 1, 2019): 10. <https://doi.org/10.1016/j.techsoc.2019.04.006>.
- Sangiovanni, Andrea. “How Practices Matter.” *Journal of Political Philosophy* 24, no. 1 (March 2016): 3–23. <https://doi.org/10.1111/jopp.12056>.
- Scientific Foresight. “Surveillance Capitalism and Europe’s Moral Duty to Shape a Human-Centric Digital Future.” European Parliamentary Research Service, January 14, 2021. <https://epthinktank.eu/2021/01/14/surveillance-capitalism-and-europes-moral-duty-to-shape-a-human-centric-digital-future/>.
- Sen, Amartya. *Inequality Reexamined*. Oxford: Oxford University Press, 1995. <https://doi.org/10.1093/0198289286.001.0001>.
- Simmons, Beth. *Mobilizing Human Rights: International Law in Domestic Politics*. Cambridge: Cambridge University Press, 2009.
- Sloan, Robert H., and Richard Warner. “Algorithms and Human Freedom.” *Santa Clara High Technology Law Journal* 35, no. 4 (March 13, 2019). <https://doi.org/10.2139/ssrn.3351960>.
- Song, Sarah. “Multiculturalism.” In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Fall 2020. Metaphysics Research Lab, Stanford University, 2020. <https://plato.stanford.edu/archives/fall2020/entries/multiculturalism/>.
- Sprankling, John G. *The International Law of Property*. Oxford: Oxford University Press, 2014. <https://doi.org/10.1093/acprof:oso/9780199654543.003.0009>.
- Stepanov, Ivan. “Introducing a Property Right over Data in the EU: The Data Producer’s Right – an Evaluation.” *International Review of Law, Computers & Technology* 34, no. 1 (January 2, 2020): 65–86. <https://doi.org/10.1080/13600869.2019.1631621>.

- Taylor, James Stacey. "Autonomy." Britannica. Accessed December 20, 2021.  
<https://www.britannica.com/topic/autonomy>.
- Teixeira, Isabel. "Digital Markets Act: Ending Unfair Practices of Big Online Platforms." Press Release. European Parliament, November 23, 2021.  
<https://www.europarl.europa.eu/news/en/press-room/20211118IPR17636/digital-markets-act-ending-unfair-practices-of-big-online-platforms>.
- "The Philosophical Foundations of Human Rights: An Overview," n.d., 38.
- "The Rise of Data Capital." MIT Technology Review Custom, 2016.  
<https://www.technologyreview.com/2016/03/21/161487/the-rise-of-data-capital/>.
- UN Office of the High Commissioner for Human Rights and League of Arab States. "Arab Charter on Human Rights," 2004, 21.
- United Nations. "Second Committee Approves 12 Resolutions, Including Texts on Eradicating Rural Poverty, Addressing Digital Divide," November 30, 2018.  
<https://www.un.org/press/en/2018/gaef3511.doc.htm>.
- United Nations. "Universal Declaration of Human Rights." United Nations. Accessed December 21, 2021. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.
- Warf, Barney. "Geographies of Global Internet Censorship." *GeoJournal* 76, no. 1 (2011): 1–23.
- Weatherford, Stephen M. "Measuring Political Legitimacy." *The American Political Science Review* 86, no. 1 (1992): 149–66. <https://doi.org/10.2307/1964021>.
- Wenar, Leif. "John Rawls." In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Summer 2021. Metaphysics Research Lab, Stanford University, 2021.  
<https://plato.stanford.edu/archives/sum2021/entries/rawls/>.
- Wike, Richard, and Katie Simmons. "Global Support for Principle of Free Expression, but Opposition to Some Forms of Speech." Pew Research Center, November 18, 2015.  
<https://www.pewresearch.org/global/2015/11/18/global-support-for-principle-of-free-expression-but-opposition-to-some-forms-of-speech/>.
- Xu, Ke, Vicky Liu, Luo Yan, and Yu Zhijing. "Analyzing China's PIPL and How It Compares to the EU's GDPR." *International Association of Privacy Professionals* (blog), August 24, 2021.  
<https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/>.
- Zuboff, Shoshanna. *The Age of Surveillance Capitalism*. New York City: PublicAffairs Books, 2018.