

## BEING HUMAN IN AN ALGORITHMICALLY CONTROLLED WORLD

Harlan Onsrud and James Campbell  
School of Computing and Information Science, University of Maine

### Abstract

Most people in developed countries, and many in developing countries, increasingly interact with Artificial Intelligence (AI) developed algorithms on an almost daily basis, yet very few are aware of those interactions or of their effect upon people's daily lives.<sup>2</sup> Using machine learning, automated reasoning, and other forms of AI, algorithms deployed in information systems take actions according to criteria set up by software developers to maximize profits regardless of the overall effects on the autonomy or welfare of individuals or on society as a whole.<sup>3</sup> The goals of the research reported here are to:

- review contemporaneous literature and quantitative economic evidence on the effects of pervasive tracking and algorithmic controls on individuals and on society in general,
- summarize a range of suggested solutions for lessening the adverse effects, and
- describe and expand upon selected legal solutions from the literature that the authors believe might place the nation on practical and more ethically defensible paths that would lead towards more equitable distribution of the benefits arising from the information economy.

**Keywords:** personal information privacy; economic inequality; surveillance capitalism; human rights

### 1. INTRODUCTION

Modern information systems gather detailed location-based, place-based, and transactional data that is aggregated, accessed, exchanged, and sold among businesses with few practical constraints except that access and transfers must be for legitimate business purposes. Persistent tracking of millions of people's locations and their contextual settings can generate, over time, surprisingly detailed information about each person in terms of who s/he is, what s/he cares about, how daily life is lived, socio-economic status, and more. Algorithmic operations applied to big data can be used to classify and target individuals to sell them goods or services more effectively, and to influence decisions and attitudes in social and political contexts. Human activity tracking and service delivery systems are not designed to support ethical concepts such as beneficence, non-maleficence, justice, and individual autonomy.<sup>4</sup> Most commercial

---

<sup>1</sup> This version posted at <https://umaine.edu/scis/beinghumanonsrudcampbellpreprint/> is the Authors Original preprint version with March 2020 additions and contains no edits made in response to journal reviewer or editor suggestions.

<sup>2</sup> H. Fry, *Hello World: Being Human in the Age of Algorithms* (New York, 2018), 3.

<sup>3</sup> D. M. West, *The Future of Work: Robots, AI, and Automation* (Washington D.C., 2018), 64-79

<sup>4</sup> T. Beauchamp and J. Childress, *Principles of Biomedical Ethics*, 6<sup>th</sup> ed. (Oxford, 2008).

information systems incorporating big data are blind to such considerations.<sup>5</sup> Rather, such systems are designed with the primary goal of maximizing profits for the owners of those systems.

Information systems that touch daily life determine and store to the greatest practical extent the physical location of each individual's actions and transactions (i.e. location-based data) in order to assess situational awareness relative to the actions and characteristics of others, objects, spaces, and institutions in close physical and virtual proximity (i.e. place-based data). By knowing detailed past actions and transactions about a person and others around that person, and by knowing the physical and virtual sites with which a person typically affiliates, AI techniques are better able to analyze past action patterns and predict an individual's future actions.

This detailed personal information at the individual and aggregate levels is extremely valuable. If an information system environment, such as Google, Amazon or Facebook, presents a user with selected information in a certain form, their AI algorithmic processes can predict that the user is statistically more likely to respond with a desired profit maximization choice or choices. The offered choices are not focused on the user's best interests. While the user often assumes that the primary objective is to provide services of value to the user, the ultimate objective of dominant information systems is to lead the user to make choices optimizing profits for the corporate owner.

These big data aggregation and decision-guidance systems are changing the bounds and conditions under which human users are able to act efficiently or, indeed, autonomously. They reduce the ability of humans to make choices and decisions as an autonomous agent, with little awareness of the growing extent to which this influencing is happening. In addition to subtly but massively changing the abilities of individuals to decide, dominant information systems, which we as researchers are complicit in advancing, are contributing to the bleeding of economic and political power away from most members of society. Through these algorithmic processes, the digital economy is changing the pragmatic reality of what it means to be human.

Information systems designed to attract and retain consumers have been engineered to perform just above the threshold that keeps the owners or corporate controllers from either civil or criminal sanctions. This currently is a very low bar that has resulted in devastating effects on large segments of the population and on society as a whole.

## **2. EXPANSION OF ECONOMIC INEQUALITY**

The spread of algorithmic information systems has had profound economic effects in addition to impacts on human agency and autonomy. The increase in economic inequality in the United States is irrefutable, and information technology has played a major role. "The system in America and around the world has been organized to siphon the gains from innovation upward such that the fortunes of the world's billionaires now grow at more than double the pace of everyone else's."<sup>6</sup> The middle class is rapidly shrinking. "... The average pre-tax income of the top ten percent of Americans has doubled since 1980, that of the top one percent has more than

---

<sup>5</sup> This blindness is closely related to or an aspect of the concept of "radical indifference" explored in S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York, 2019) 504-512.

<sup>6</sup> A. Giridharadas, *Winners Take All: The Elite Charade of Changing the World* (New York, 2018), 5.

tripled, and that of the top .001 percent has risen more than sevenfold”.<sup>7</sup> Over the same time period, the pretax average income of the lower half of Americans, adjusted for inflation, rose from \$16,000 in 1980 to only \$16,200 in 2014.<sup>8</sup> While the nation experienced over thirty years of stunning technological advancements supporting a robust information economy, the benefits from those advancements resulted in virtually no effect on the average wages for 117 million Americans.<sup>9</sup> Only 50% of Americans born in the 1980s can expect to earn more than their parents.<sup>10</sup>

It is asserted that the middle and working classes depend primarily upon annual income to support their standard of living while the rich tend to rely on accumulated wealth and the investment returns it provides, distinguishing them from the vast remainder of the population.<sup>11</sup> “The top one-tenth of 1 percent now owns almost as much wealth as the bottom 90 percent.”<sup>12</sup> Professor Robert Reich makes the case that income inequality is now the defining issue in the United States.<sup>13</sup> He points out that “95 percent of economic gains since the “so-called” recovery started in 2009 have gone to the top 1 percent by net worth.”<sup>14</sup> Emmanuel Saez, as well, reported that in the first three years of the recovery, the top 1% captured 91% of income gains.<sup>15</sup> In 2017, it was widely reported that the wealthiest 3 billionaires in the U.S. – Jeff Bezos, Bill Gates and Warren Buffett — had now acquired as much wealth as the bottom half of the U.S. population combined.<sup>16</sup> Similar recent national and global statistics are abundant. An earlier study by the Harvard Business School published in 2014 made the point that there is a troubling and growing divergence of the very wealthy from the working class, middle class, and small businesses that is no longer sustainable.<sup>17</sup>

To date, “Half the decline in workers’ share of income in the developed world can be attributed to advancing technology.”<sup>18</sup> In many fields, technology is substituting for labor.<sup>19</sup> This reality is

---

<sup>7</sup> Giridharadas, *Winners Take All*, 4, 16. The top 1% average pre-tax income was \$1.3 million/year in 2014 versus \$428,000 in 1980 adjusted for inflation and the top .001 percent average pre-tax income had risen to \$122 million/year by 2014.

<sup>8</sup> Giridharadas, *Winners Take All*, 16.

<sup>9</sup> Giridharadas, *Winners Take All*, 4.

<sup>10</sup> West, *The Future of Work*, 138.

<sup>11</sup> D. Gilbert, *The American Class Structure: In an Age of the Growing Inequality* (Belmont CA, 1998)

<sup>12</sup> Emmanuel Saez and Gabriel Zucman, *Wealth Inequality in the United States since 1913: Evidence from Capitalized Income Tax Data*, National Bureau of Economic Research (NBER) Working Paper No. 20625, Issued in October 2014, <http://www.nber.org/papers/w20625> and <https://www.nber.org/papers/w20625.pdf>

<sup>13</sup> A. Svaldi, ‘Robert Reich: Income inequality the defining issue for U.S.’ *Denver Post* (11 Jan 2014) <https://www.denverpost.com/2014/01/10/robert-reich-income-inequality-the-defining-issue-for-u-s/>, last accessed 13 Feb 2020.

<sup>14</sup> Svaldi, n.p.. Also see J. Kornbluth, *Inequality for All* (2014), <http://inequalityforall.com/>

<sup>15</sup> E. Saez, *Striking it richer: The evolution of top incomes in the U.S.* (Berkeley CA, 2016) <https://eml.berkeley.edu/~saez/saez-UStopincomes-2015.pdf>, last accessed 13 Feb 2020

<sup>16</sup> Institute for Policy Studies, <https://ips-dc.org/wp-content/uploads/2017/11/BILLIONAIRE-BONANZA-2017-FinalV.pdf>, , last accessed 13 Feb 2020

<sup>17</sup> M. Porter and J. Rivkin, *An Economy Doing Half Its Job: Findings of Harvard Business School’s 2013–14 Survey on U.S. Competitiveness* (Boston, 2014) 2. <https://www.hbs.edu/competitiveness/documents/an-economy-doing-half-its-job.pdf/>, last accessed 13 Feb 2020.

<sup>18</sup> M. Schuman, ‘Why Wages Aren’t Growing’, *Bloomberg Businessweek*, (25 Sept 2017), <https://www.bloomberg.com/news/articles/2017-09-21/why-wages-aren-t-growing>, last accessed 23 May 2019

<sup>19</sup> West, *The Future of Work*, 67.

having dramatic consequences for middleclass jobs.<sup>20</sup> The evidence is mounting that technology is destroying many existing jobs while at the same time creating some new jobs at the high and low ends of the wage spectrum, but many fewer good jobs in the middle.<sup>21,22</sup>

Historically, small businesses have generated a high proportion of new jobs and economic opportunity in the US. While one might assume that the increased communication capabilities of today would make it much easier to start a business, “the number of new firms launched each year has fallen by nearly two-thirds since 1980”<sup>23</sup> and “... the share of young people who own a business has fallen by two thirds” during the same time period.<sup>24</sup> “Between 2005 and 2015, the number of small retailers fell by 85,000, a drop of 21 percent relative to population” and the long-standing path to the middleclass of starting a business is increasingly being lost.<sup>25</sup>

The current problem in the U.S. is not so much unemployment as massive underemployment. Even highly educated individuals lacking high level information age skills are underemployed in low paying jobs. Such workers are now often hired as part-time and temporary independent contractors “as needed” rather than as employees in order to avoid paying benefits.<sup>26</sup> Job prospects for these individuals will continue to worsen without substantial societal realignments.

The legal system in the U.S. and agreements with other nations have rewarded innovation and investment for those at the top at the expense of broader populations. Globally, the top ten percent of humanity now controls 90 percent of the planet’s wealth.<sup>27</sup> As expressed by economist Daron Acemoglu and political scientist James Robinson in 2012:

“So here is the concern, economic inequality will lead to greater political inequality, and those who are further empowered politically will use this to gain greater economic advantage, stacking the cards in their favor and increasing economic inequality still further – a quintessential vicious circle. And we may be in the midst of it.”<sup>28</sup>

Through massive data accumulation and algorithmic mining, supported by anti-monopoly law shifts by the Supreme Court so that the law now focuses on efficiency and pricing with little regard for the stifling and elimination of competitors, Amazon has created a commerce infrastructure capturing “nearly \$1 out of every \$2 that Americans spend online”<sup>29</sup> thereby dwarfing the breadth, depth, and size of monopolistic financial empires that were disbanded in past times under previous interpretations of U.S. antitrust law.

---

<sup>20</sup> West, *The Future of Work*, 67-68, 153.

<sup>21</sup> D. Rotman, ‘Who Will Own the Robots’, MIT Technology Review (Sept 2015), <https://www.technologyreview.com/s/538401/who-will-own-the-robots/>, last accessed 23 May 2019

<sup>22</sup> M. Muro, S. Liu, J. Whiton, and S. Kulkarni, ‘Digitalization and the American Workforce,’ Metropolitan Policy Program, Brookings Institution (Nov 2017), [https://www.brookings.edu/wp-content/uploads/2017/11/mpp\\_2017nov15\\_digitalization\\_full\\_report.pdf](https://www.brookings.edu/wp-content/uploads/2017/11/mpp_2017nov15_digitalization_full_report.pdf), last accessed 23 May 2019

<sup>23</sup> S. Mitchell, ‘Amazon Doesn’t Just Want to Dominate the Market – It Wants to Become the Market’, *The Nation* (15 Feb 2018) 1-28, Cited here at 13. <https://www.thenation.com/article/amazon-doesnt-just-want-to-dominate-the-market-it-wants-to-become-the-market/>, last accessed 23 May 2019.

<sup>24</sup> Giridharadas, *Winners Take All*, 3

<sup>25</sup> Mitchell, ‘Amazon Doesn’t Just Want to Dominate the Market’, 12-13 and West, *The Future of Work*, 141.

<sup>26</sup> West, *The Future of Work*, 66, 79, 81, 108

<sup>27</sup> Giridharadas, *Winners Take All*, 5.

<sup>28</sup> E. Brynjolfsson and A. McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (New York, 2014), 172.

<sup>29</sup> Mitchell, ‘Amazon Doesn’t Just Want to Dominate the Market’, 5.

Large companies able to attract very large user bases with continually updated daily streams of data from their users, and the ability to integrate that data with historic individualized transactions and location data, have a highly competitive market advantage. Typically, these companies ensure that their actions are not in violation of existing laws protecting personal privacy. However, such laws in the U.S. are in narrowly defined thematic areas<sup>30</sup> and are often clearly bounded so the corporate burden in meeting them is not insurmountable. Such companies also ensure that acquisition and sharing is accomplished for legitimate business purposes. However, since companies themselves largely define what is legitimate, this again causes little burden. Further, companies ensure that information tied to identity is kept confidential by contract among sharing businesses. This is accomplished primarily to protect the trade secret rights of the involved companies as opposed to protecting the privacy of data subjects, which it also happens to accomplish in part. Further, such businesses ensure that the sharing is not in violation of the business's own privacy protection policies. However, this business burden is also minimized typically by ensuring that policies are self-written and often use purposeful obfuscation so that users are unlikely to read them or understand the full ramifications before clicking their concurrence.

If the above practices are followed, companies are generally comfortable in acquiring data by sale, license, barter, trade, or otherwise from other businesses. This digital business environment supported by current law makes massive accumulation of data possible that can reliably profile the interests and predict the economic and social behavior of hundreds of millions of individuals and, concurrently, make massive wealth concentration possible.

Meeting only the low bar of current laws has resulted in substantial economic and legal inequalities harming the overall well-being of most members in modern digital societies. The legal bars need to be raised to serve higher and broader human and societal needs.

### **3. EFFECTS OF MACHINE MINING OF LOCATION-BASED AND PLACE-BASED BIG DATA**

Access to massive “big data” enables predictive analytics and other AI techniques. The correlations and patterns that AI techniques uncover typically cannot be spotted by humans nor are the resulting machine-derived algorithms even understood by the humans that developed the original software.

For example, while a machine learning system might typically incorporate no theory as to why substantially more users with certain location and transaction characteristics and habits similar to a particular person click on a web link when a different word, phrase, image or color is presented, the AI might simply recognize the pattern as significant and alter the view appropriately to maximize a person's likelihood in making a favorable selection.

Information systems are increasingly running successions of A versus B testing scenarios in order to determine and offer a user options or views to which users similar to that user have been most likely to respond positively in the past.<sup>31</sup> Continual scenario testing to facilitate machine learning by presenting different web views to control and test groups of users thousands of times throughout each day as customers interact with sites is already quite

---

<sup>30</sup> For a sampling of thematic privacy laws germane to information professionals and summaries of them, consult C. Givens, *Information Privacy Fundamentals for Librarians and Information Professionals* (Lanham MD, 2014), 31-46.

<sup>31</sup> Stevens-Davidowitz, *Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are* (New York 2017), 209-221.

common and growing rapidly. The correlations and statistical predictions resulting from machine learning and other AI techniques have proven to be highly effective in leading humans to make choices that maximize profits for corporate controllers, regardless of the impact on individual humans. In Zuboff's words, users are "herded" into making those choices.

While the machine-derived algorithms arising from the mining of massive data collections have been successful in directing human actions to maximize profits, such algorithms have also come under severe criticism. AI has been shown to discriminate against certain groups through its analysis of finely parsed data. Because massive data collections often reflect current and past discriminatory practices, machine learning inevitably incorporates those biases into choices offered to individuals. The discrimination becomes embedded almost invisibly into the automated systems.

For example, some users of B&B room reservation systems with distinctly sounding African-American names have been less likely to be accepted as guests at certain establishments.<sup>32</sup> If machine recognition picks up such a pattern, it will typically affect guest rental offerings to future parties with similar names. This has the effect of embedding discriminatory practices in offerings even though it may not have been the intent of the software designers or a corporate entity to constrain offers in such a manner.

Other documented examples include automated discrimination against women in executive searches, rejection of identification of dark-complexioned parties through facial recognition software, and adverse offer decisions based on automated guilt-by-association machine profiling in regard to loan, insurance, and school admission applications as well as crime risk and recidivism predictions.

Should corporate developers and users of AI be held legally accountable if they have no explicit idea how algorithms are operating in controlling their information systems except that they work exceptionally well in soliciting responses from users that maximize their corporate profits? Do, or should, they have a legal obligation to explore adverse effects of their information systems on individuals and society as a whole?

Cathy O'Neill argues that algorithmic decision-making will inevitably become much more ubiquitous in the future and society must demand that auditing systems that hold such systems accountable must become ubiquitous as well. She argues that results from automated decision-making must be legal, fair, and grounded in fact.<sup>33</sup> How to deploy and enforce such capabilities is not clear although efforts are beginning to attempt to better understand these processes.<sup>34</sup>

In the future, machines will additionally estimate our emotions as we view information or images on screens using camera views of our live facial expressions, vocal intonation patterns, and other signals as further input into assessing suitability for product offerings, or susceptibility to social decisions up to and including voting in elections.<sup>35</sup> That is, if your face indicates you are frowning or questioning the text you are reading currently or the audio you are hearing, you will

---

<sup>32</sup> West, *The Future of Work*, 36.

<sup>33</sup> C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York, 2016), 231.

<sup>34</sup> See e.g. R.Gordon, 'Building AI systems that make fair decisions', *MIT News* (April 24, 2018), <https://news.mit.edu/2018/building-ai-systems-that-make-fair-decisions-harini-suresh-0424>, last accessed 23 May 2019.

<sup>35</sup> West, *The Future of Work*, 35-39.

be sent one next written message, ad, or video whereas those smiling or agreeing with the screen message will be next sent an alternative message.

Numerous further bio-feedback systems are on the horizon. In the future, your cell phone will have embedded within it an "electronic nose" more sensitive than any dog nose.<sup>36</sup> Dogs are being trained successfully in experimental settings to detect human diseases by smell alone such as for prostate cancer, colorectal cancer, diabetes, Parkinson's, tuberculosis, malaria, and urinary tract infections. Through the ability of trained dogs to smell malignant tissues, algorithms for use with artificial bioelectronic noses are then being trained using AI techniques to identify the same smells.<sup>37</sup> One related future goal is that a range of "wearables", with very small sensors embedded within and helping to form the yarn of fabric, will use much smarter algorithms to allow internet-enabled fabrics to achieve detailed, comprehensive, and unobtrusive biometric monitoring of individuals.<sup>38</sup> Early diagnosis of maladies could be greatly improved leading as well to early and more effective treatment. While promising great benefits, these and myriad similar emerging tracking technologies are certain to give rise to increased legal, ethical, and economic concerns if society continues on its current course in failing to support and enable the autonomy of individuals to effectively control their own information exposure.

A survey of AI experts conducted by researchers at Yale and Oxford predicts that there is a 50% chance that AI will outperform humans in all tasks within 45 years.<sup>39</sup> Workers in almost all major sectors will lose jobs, including those engaged in waiting tables, working in retail, driving, writing, analyzing, coding, manufacturing, educating others, diagnosing and treating diseases, and conducting surgery. No current employment sector will be untouched. Forty-seven percent of U.S. workers have a high probability of having their jobs automated over the next 20 years.<sup>40</sup>

For most people, work is not only economically necessary, work adds value to human self-worth. It adds purpose. "Purpose is that sense that we are part of something bigger than ourselves, that we are needed, that we have something better ahead to work for. Purpose is what creates true happiness."<sup>41</sup> While purpose may be gained by activities other than work, loss of work is, and will continue to be, alienating for those affected.

"The inability of the U.S. economic and political system to address basic problems angers ordinary citizens and intensifies mistrust in democratic institutions."<sup>42</sup> If the U.S. economic situation is left as is, scholars are predicting much greater "increases in income inequality, massive numbers of people who are effectively unemployable, and breakdowns in the social order."<sup>43</sup>

---

<sup>36</sup> S. Harrison, 'The Quest to Make a Bot That Can Smell as Well as a Dog' *Wired* (16May2020) n.p., <https://www.wired.com/story/quest-to-make-robot-smell-cancer-dog/>

<sup>37</sup> M. Molteni, 'The Science of the Sniff: Why Dogs Are Great Disease Detectors' *Wired* (30Oct2018) n.p., <https://www.wired.com/story/the-science-of-the-sniff-why-dogs-are-great-disease-detectors/>

<sup>38</sup> Zuboff, *The Age of Surveillance Capitalism*, 246.

<sup>39</sup> West, *The Future of Work*, 68.

<sup>40</sup> West, *The Future of Work*, 70.

<sup>41</sup> M. Zuckerberg, 'Full Text of Mark Zuckerberg's Harvard Graduation Speech', *USA Today* (25 May 2017) <https://www.usatoday.com/story/tech/news/2017/05/25/mark-zuckerberg-harvard-graduation-speech-facebook/102158466/>, last accessed 23 May 2019.

<sup>42</sup> West, *The Future of Work*, 138.

<sup>43</sup> A. Smith and J. Anderson, 'AI, Robotics, and the Future of Jobs', Pew Research Center (6 Aug 2014), 5, <https://www.pewresearch.org/wp-content/uploads/sites/9/2014/08/Future-of-AI-Robotics-and-Jobs.pdf>, last accessed 23 May 2019.

#### 4. PERSONAL LOCATION DATA PRIVACY CHALLENGES

A recent study showed that "privacy and security of personal information and data is the second most worrisome issue to consumers behind healthcare." (Richard Whitman, Consumers Worry More About Privacy than Any Other Issue Except Healthcare) One class of data use identified as particularly intrusive is the continual tracking of location data. Location data on individuals is a very large and growing business. Location data about smartphone users "... is being traded on an increasingly robust secondary market, often without your knowledge. According to a New York Times investigative report, your precise location can be traced up to 14,000 times per day. .... Currently more than 1,000 apps contain location-sharing code and the current size of the location-targeted advertising market is \$21 billion."<sup>44</sup>

"There is no known effective method to anonymize location data, and no evidence that it's meaningfully achievable."<sup>45</sup> While data brokers may argue that data being traded is anonymous since it typically is not tied to a unique human name, phone number or social security number, all locations recorded by a particular device owned or operated by a human are typically tied to an ID for that device. In 2013, MIT and Belgian researchers "analyzed data on 1.5 million cellphone users in a small European country over a span of 15 months and found that just four points of location reference, with fairly low spatial and temporal resolution, was enough to uniquely identify 95 percent of them."<sup>46</sup> That is, out of millions of travel paths accumulated each year within any regional area, knowing only a few locations that a specific person frequents (e.g. home, school, office, regular purchaser at a particular grocery store, etc.) results in a very high probability of identifying the person that is carrying or driving the tracked device or vehicle. Thus, the number of device or vehicle trips taken, when they were taken, the exact travel paths taken, their durations, and who is highly likely to have traversed the paths are readily determinable.

As Paige Boshell concludes:

- identified location data is regularly acquired and used by third parties with whom the individual has no direct relationship;
- de-identified or anonymized location data is regularly re-identified; and
- location data is routinely combined with other types of personal data and used by third parties with whom the individual has no direct relationship to compile comprehensive profiles of the individual and make decisions about the individual or attempt to influence behavior of the individual.

These secondary-market practices are not currently addressed by United States law.<sup>47</sup>

Consumers typically have the ability to shut off the use of GPS capabilities on their smart phones for their various applications. However, most fail to do so because they probably bought the phone in the first place to accomplish at least some tasks that rely on their location. Further, in 2017, investigative reporters discovered and reported that "Android phones had been

---

<sup>44</sup> N. Lindsey, The Big Business of Location Data, *CPO Magazine* (20 Jan 2019), <https://www.cpomagazine.com/data-privacy/the-big-business-of-location-data/>, last accessed 15 March 2020.

<sup>45</sup> Zuboff, *The Age of Surveillance Capitalism*, 245-246.

<sup>46</sup> P. Boshell, The Power of Place: Geolocation Tracking and Privacy, *Business Law Today* (25 March 2019) 15, <https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/> citing L. Hardesty, How hard is it to "de-anonymize" cellphone data? MIT News (27 March 2013)

<sup>47</sup> Boshell, The Power of Place, 47

collecting location information by triangulating the nearest cell towers, even when location services were disabled, no apps were running, and no carrier SIM card was installed in the phone."<sup>48</sup> In addition, numerous companies are reporting indoor location tracking advancements combined with GPS tracking including Broadcom that reported in 2012 that it had created a global positioning capability "... in a chip that combines satellite communications with the sensors in your cell phone to create a "positioning engine" that can find your location even if you are not connected to a network, including your location in a building, how many steps you've taken, in what direction, at what altitude."<sup>49</sup> Further, your device ID and location are automatically embedded in any photos or videos you take. It is suspected that many free game apps exist for the sole purpose of acquiring where and when users are at for the sole purpose of selling that data on the secondary market. "Most smartphone apps demand access to your location even when it's not necessary for the service they provide, simply because the answer to this question is so lucrative."<sup>50</sup>

Thus, even if a consumer chooses to opt out of use of location tracking for specific applications, the fine print to which consumers click agreement may very well allow continued use of location tracking for many other purposes such as to maintain and expand the very large data streams that feed AI techniques and make them so powerful. Machine-learning algorithms, also known as "learners", make inferences from examples reflected in data to arrive at typically automated responses, actions, or recommendations. The more data learners have to analyze, the better they get in recognizing patterns and making predictions that no human would be able to match. As succinctly stated by Pedro Domingos, "Whoever has the best algorithms and most data wins."<sup>51</sup> Thus, there is a very strong incentive for corporations to track user locations and other data provided by embedded sensors even if consumers decline to use the location apps available to them on their smart phones and other carried devices.

## 5. SURVEILLANCE CAPITALISM

Shoshana Zuboff argues that the world has reached the beginnings of a new, original, and unprecedented age of surveillance capitalism.

Surveillance capitalism unilaterally claims human experience as free raw materials for translation into behavioral data. Although some of these data are applied to product or service improvement, the rest are declared as a proprietary *behavioral surplus*, fed into advanced manufacturing processes known as "machine intelligence", and fabricated into *prediction products* that anticipate what you will do now, soon and later. Finally, these prediction products are traded in a new kind of marketplace for behavioral predictions that I call *behavioral futures markets*. Surveillance capitalists have grown immensely wealthy from these trading operations ...<sup>52</sup>

---

<sup>48</sup> Zuboff, *The Age of Surveillance Capitalism*, 244 citing Keith Collins, "Google Collects Android Users' Locations Even When Location Services Are Disabled," *Quartz* (21 Nov 2017), <https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled>

<sup>49</sup> Zuboff, *The Age of Surveillance Capitalism*, 244 citing Christina DesMarais, "This Smartphone Tracking Tech Will Give You the Creeps," *PCWorld*, May 22, 2012, [http://www.pcworld.com/article/255802/new\\_ways\\_to\\_track\\_you\\_via\\_your\\_mobile\\_devices\\_big\\_brother\\_or\\_good\\_business\\_.html](http://www.pcworld.com/article/255802/new_ways_to_track_you_via_your_mobile_devices_big_brother_or_good_business_.html)

<sup>50</sup> Zuboff, *The Age of Surveillance Capitalism*, 242.

<sup>51</sup> P. Domingos, *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World* (New York, 2015) 12

<sup>52</sup> Zuboff, *The Age of Surveillance Capitalism*, 8.

The goal is no longer "... to automate information flows *about us*; the goal is to *automate us*." The power of this unprecedented economic, political, and social instrumentation that affects everyone is to know and shape "... human behavior towards others ends."<sup>53</sup> The aim is to dominate human nature.

Just as industrial civilization flourished at the expense of nature and now threatens to cost us the Earth, an information system shaped by surveillance capitalism and its new instrumentation power will thrive at the expense of human nature and will threaten to cost us our humanity.<sup>54</sup>

Democracies demand the right of peoples to self-govern. There is no single form of democracy and no single form of capitalism. Democracies adjust through legislative and judicial actions over time in response to public opinion about injustices and oppression. Capitalism adjusts over time through altered means for generating wealth in order to meet new needs. Surveillance capitalism is not and should not be inevitable or inviolable. "It is not OK for every move, emotion, utterance, and desire to be catalogued, manipulated, and then used to surreptitiously herd us through the future for the sake of someone else's profit. 'These things are brand new.' ... They are unprecedented."<sup>55</sup> Corrective laws and jurisprudence are still possible. New forms of ownership and methods of production may be created.

## 6. SUGGESTED SOLUTIONS

On an economic level, a fundamental research question for our algorithmic era is how information societies can enable rich opportunities for all humans to more equitably share in the economic benefits of information technology rather than funneling the benefits upwards towards those individuals with greatest existing wealth. The literature suggests corrective actions that might place societies across the globe on paths leading to improved economic gains for all. Some of the suggested reforms are decades old while others are newly emerging.

Means for dealing with inequitable societal and human consequences caused by technological advancements and changing business models have included a range of suggested approaches for ensuring sustained worker income and benefits, and a range of revenue generation approaches to pay for such benefits. Among innovative programs suggested for ensuring smoother transitions for workers in moving through successive jobs over a lifetime have included:

- citizen accounts able to accrue benefits outside of and across jobs,
- widespread implementation of paid family and parental leave,
- universal health care,
- remunerating work of value to society not currently accounted for such as parenting, volunteering, and mentoring,
- expansion of the earned income tax credit approach to help the working poor,
- providing free college,
- providing free lifelong distance learning in critical needs areas,
- providing universal basic income as a safety net for all citizens, and
- similar programs.<sup>56</sup>

---

<sup>53</sup> Zuboff, *The Age of Surveillance Capitalism*, 8.

<sup>54</sup> Zuboff, *The Age of Surveillance Capitalism*, 11.

<sup>55</sup> Zuboff, *The Age of Surveillance Capitalism*, 521.

<sup>56</sup> West, *The Future of Work*, 89 -102.

Suggested proposals to pay for such programs have included raising income taxes on those in the top 1% of earners, applying a progressive tax on high consumption goods purchased typically only by the very wealthy, applying a solidarity tax on net assets owned by high-worth individuals, applying a graduated tax on wealth, and cutting back on some tax-funded social programs.<sup>57</sup>

All of the benefit and safety net programs suggested and the revenue generation approaches proposed to pay for them have strengths, drawbacks, and different likelihoods of success. Many of the approaches have already been tested in national or local government contexts across the globe. While the details of these proposals and the methods to pay for them are too lengthy to summarize here, some combination of these and additional approaches are likely to be applied in the U.S. in the future as income inequality and societal disruptions become more pronounced.

Economic livelihood is critically important to human existence: so are factors like autonomy and agency. Having control over one's personal life and decisions requires a level of privacy which is difficult to maintain in an increasingly algorithmically controlled world. Efforts to rebalance the power of individual personal privacy choice versus big data information systems have been introduced by a variety of actors. "Privacy by Design," for example, is a framework initiative initially developed by the Information and Privacy Commissioner of Canada and adopted by the International Assembly of Privacy Commissioners and Data Protection Authorities in 2010<sup>58</sup>. It basically advocates for privacy to be an element of software system design from inception to deployment and beyond, rather than being tacked on as an afterthought, if privacy is considered at all. Another approach championed by groups such as the American Association for the Advancement of Science (AAAS) and security expert Bruce Schneier advocate for experts in computing and scientific fields to serve on a short-term basis with government and, in some cases, corporate entities to bring technical expertise to the process of legislation creation and of corporate governance and practice. Privacy considerations could become part of those initiatives which would consider the effects of data collection on human autonomy and agency as legislation and corporate policies are developed.

## 7. LEGAL FOUNDATIONAL ADJUSTMENTS

Some suggest that it is primarily low legal bars that are resulting in inordinate wealth concentration for the few. Inadequacies of our laws expose society to increasing threats to liberty and undermining of the operations of democratic governments. These scholars suggest that it is foundational laws that should be altered to allow more equitable distribution of the profits and other benefits that are being accrued from technological advancements, including the proliferation of big data predictive technologies discussed above. Reward systems should be straightened out at their foundations through application of the law rather than addressing a plethora of adverse ramifications one-by-one. Using this approach, proponents suggest, would result in much less need to provide social safety nets for middle-class and low-income earners.

One approach focuses on political reform by strengthening democratic processes, providing equal voices for ordinary citizens, and reducing polarization in politics. If politics were brought into better alignment with democratic representation and processes, then continuing

---

<sup>57</sup> West, *The Future of Work*, 102 -108.

<sup>58</sup> 32<sup>nd</sup> Annual Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy by Design* (Jerusalem, 2010), [https://edps.europa.eu/sites/edp/files/publication/10-10-27\\_jerusalem\\_resolutionon\\_privacybydesign\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf), last accessed 23 May 2019.

compromises through political processes would better lessen unjust inequities in society. Among reforms suggested in this arena in the U.S. include:

- legislation or constitutional reforms that would far better enable control by individuals over their personal information exposure,<sup>59</sup>
- substantive campaign finance reform which, as a prerequisite, would require a constitutional amendment to overturn *Citizens United v. Federal Election Commission*, 558 U.S. 310 (2010)
- adaptation and tougher enforcement of antitrust law to protect citizens and competing businesses from the adverse effects of monopolies as opposed to the current state of supporting antitrust law primarily as a technical tool to maximize efficiency and keep prices low,<sup>60</sup>
- dampening political polarization by supporting ranked-choice voting,
- dampening political polarization by requiring all citizens to vote or face a civil fine so that a much larger percentage of less politically fervent citizens vote,
- reforming partisan redistricting,
- reforming the electoral college or eliminating it since it is increasingly misaligned with population distribution, and
- similar myriad proposals introduced in Congress each year.

A further category of corrective foundational laws includes those that would grant much stronger *human rights* in personal private data over the competing legal rights of corporations and other socially constructed entities. It is this latter category on which the remainder of this paper is focused.

## 8. REVISITING HUMANISTIC INFORMATION ECONOMY AND LEGAL APPROACHES

The core of this work revisits innovative reforms offered by leading legal scholars when the Internet and information economy were yet nascent and forming. Here we focus on two independent but complementary approaches that were largely dismissed when originally proposed as politically inexpedient or as too impractical considering the state of technology at the time.

The initiating scholars referenced here are now deceased. Had either or both of the suggested paths been followed, U.S. society might have reached the highly robust information economy that we have today but with much better protection of personal information privacy, and more equitable spreading of the increased benefits of the information economy across a far broader swath of humanity. Major advancements in technology make these approaches much more achievable than when originally proposed. With economic inequalities predicted to be greatly exacerbated if current information economy policies and laws continue unchanged, it is time for these previously dismissed and complementary approaches to be reconsidered.

---

<sup>59</sup> Specific to location data, Paige Boshell suggests a range of potential legal approaches to consider in controlling the use of location data and the potential benefits and drawback of each approach. [Boshell, *The Power of Place*, n.p.]

<sup>60</sup> A broad range of legal and economic theorists argue that, in addition to protecting consumers and overall efficiency, antitrust statutes were intended to and should also control economic power in the public interest. Judge Robert Bork, the "Chicago School of economics," and additional law and economics thinkers were successful in causing a shift in the U.S. Supreme Court's approach to antitrust laws since the 1970s to be focused solely on what is best for the consumer rather than focused on company practices and their effects on wider public interests. [R. Bork, *The Antitrust Paradox* (New York, 1978) (Second edition 1993)]

***A New Birth for Human Rights:*** Professor Charles L. Black, Jr. became a law professor in 1947 and had a long and distinguished career as a constitutional law scholar. Over his thirty-one-year career at Yale he "made Yale Law School one of the world's leading centers for the study of constitutional law."<sup>61</sup> When in his eighties, he reemerged from retirement to write a short book in 1997 containing a comprehensive yet concise set of constitutional reasoning "for the sake of all of our grandchildren." In it he states that "(t)he foundations of American human-rights law are in bad shape"<sup>62</sup> and then sets forth meticulously "... the construction of a better system of reason for the grounding of constitutional human rights in this country."<sup>63</sup>

He critiques severely and systematically the judicial reasoning of past Supreme Courts in misinterpreting the nation's founding documents in extending the Bill of Rights to corporations.<sup>64</sup> He argues that the nation's juristic founding documents provide for strong recognition of human rights and should have been interpreted to temper the power of corporations. Instead, the corporate right of "free speech" has been extended progressively by successive courts to disadvantage the constitutional privacy rights of U.S. citizens. Even Congress now has few legislative tools it may use in limiting the massive accumulation, trade, and sale of private personal data occurring among businesses.

Black sets out "the thesis that a sound and satisfying foundation for a general and fully national American law of human rights exists in three imperishable commitments – the Declaration of Independence, the Ninth Amendment, and the "citizenship" and "privileges and immunities" clauses of Section 1 of the Fourteenth Amendment (*as those clauses ought to have been and still ought to be interpreted.*)" (Emphasis added)<sup>65</sup>

In highly abbreviated form, Black summarizes his arguments as:

1. The 1776 Declaration of Independence commits all governments in our country to 'securing' for its people certain human rights, 'among which are life, liberty, and the pursuit of happiness.' ...
2. The 1791 Ninth Amendment to the Constitution is unmistakably 'law,' and unmistakably rejects the idea that a human right, to be valid in law, must be enumerated (or explicitly named). The Amendment does not say which rights are the 'others retained by the people' .... But the Declaration of Independence, uttered a mere thirteen years earlier, supplies this lack in major part. There is no apter reference than the Declaration for clearing up the words "retained by the people," whether the Declaration itself be 'law' or not." ...
- “3. The 'citizenship' and the 'privileges and immunities' clauses of Section 1 of the Fourteenth Amendment form a complex whole.”<sup>66</sup>

---

<sup>61</sup> Wikipedia, *Charles Black (professor)*, [https://en.wikipedia.org/wiki/Charles\\_Black\\_\(professor\)](https://en.wikipedia.org/wiki/Charles_Black_(professor)), last accessed 23 May 2019.

<sup>62</sup> Black, Charles L., Jr., *A New Birth of Freedom: Human Rights, Named and Unnamed*, (New York, 1997), 1

<sup>63</sup> Black, *A New Birth of Freedom*, 4

<sup>64</sup> "Today, corporations have nearly all the same rights as individuals: freedom of speech, freedom of the press, religious liberty, due process, equal protection, freedom from unreasonable searches and seizures, the right to counsel, the right against double jeopardy, and the right to trial by jury, among others." A. Winkler, *We the Corporations: How American Businesses Won Their Civil Rights*, (New York, 2018), xvi

<sup>65</sup> Black, *A New Birth of Freedom*, ix

<sup>66</sup> Black, *A New Birth of Freedom*, 38

Black argues that the phrase “life, liberty, and pursuit of happiness” must refer to living, breathing humans created by nature. Corporations do not live. Corporations as socially constructed or legally defined entities are created by filing information with the government and do not “live” in any reasonable meaning of the word. Nor may corporations be imprisoned and, hence, such entities may not be granted or enjoy liberty. Finally, as non-living legally constructed entities, corporations cannot be happy. The Declaration of Independence must have referred to humans and thus also to the inalienable rights of humans. These human rights should not have been imbued in non-human entities such as socially constructed corporations. Professor Black argues that it is not yet too late for the Supreme Court to change course and interpret the Constitution as the founding fathers intended when written.

One result of the current U.S. Supreme Court’s interpretation is, for example, that Congress would likely be banned from passing laws that force online and data processing businesses to use “opt in” business models with people that use their services as opposed to using “opt out” models.<sup>67</sup> Joseph Tomain presents strong legal arguments based on the Constitution and its interpretation through past case law for the validity of opt-in laws. Nonetheless, he believes a current majority of the U.S. Supreme Court would not uphold legislation requiring an opt-in approach for data processing and data mining commercial activities but would instead continue to expand protection for commercial free speech.<sup>68</sup>

Commercial enterprises have strong financial incentives to discourage consumers in every way from taking steps to avoid data collection. As a result, privacy policies are often overly broad, typically vague and often hidden.<sup>69</sup> The means by which users are tracked are also purposefully hidden to avoid detection.<sup>70</sup> Few, if any, companies in the era of big data are likely to use an opt-in approach voluntarily.

However, assume that opt-in requirements are allowed to be Constitutionally imposed by a future court. Assume further that legislation is passed that requires that each and every human being must now explicitly agree to terms allowing the data collected from them by each data system with which they interact in order for the data to be processed. Would this provide a solution to the problems identified above? Probably not.

When users “consent” to opt-in by volitionally responding to click-through-licenses on the many hundreds of web sites they may use, their consent can hardly be construed as “informed.” To hold so would be a legal fiction. No typical human being in navigating modern daily life could, from a practical perspective, actually read and understand all of the licenses they have been enticed, or forced, to click.<sup>71</sup>

---

<sup>67</sup> U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999). In this case, an opt-in requirement was analyzed under the doctrine of commercial free speech and held to violate the First Amendment rights of the commercial company. For legal arguments that might be used by future courts as a basis to allow imposition of opt-in requirements on the commercial sector as one element in protecting the privacy of those being tracked, consult J. A. Tomain, ‘Online Privacy and the First Amendment: An Opt-In Approach to Data Processing’, *University of Cincinnati Law Review*, 83 (2014), 1-73, <https://www.repository.law.indiana.edu/facpub/2649>, last accessed 23 May 2019.

<sup>68</sup> Tomain, ‘Online Privacy and the First Amendment’, 63-64.

<sup>69</sup> Tomain, ‘Online Privacy and the First Amendment’, 12.

<sup>70</sup> Tomain, ‘Online Privacy and the First Amendment’, 25.

<sup>71</sup> Two Carnegie Mellon researchers calculated in 2008 that reading all of the privacy policies encountered annually by an average Internet user would take 76 eight-hour work days to accomplish. [A. Madrigal, ‘Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days,’ *The Atlantic* (1 March 2012), n.p., <https://www.theatlantic.com/technology/archive/2012/03/reading-the->

The typical wording of such licenses is notoriously broad and vague. Users have no viable option to negotiate different terms even if they take on the herculean effort to read and fully understand most of the licenses they encounter in their daily use of phones, computers, other devices, and the myriad information systems they encounter through the use of their devices. Substantive choice of terms for users, particularly in the use of dominant information systems, is not really an option.

Regardless of the license terms clicked, users have little choice but to have their actions commoditized to the benefit of service providers and typically are subjected to expansive potential or actual privacy invasive behavior not banned by the overly broad terms. It is difficult to know exactly how personal data is being processed because such processing is protected by the firms doing the processing using trade secrets, often opaque technology, and other means.

In addition, “there is no longer such a thing as individually “opting out” of our privacy compromised world.” ... “Because of technological advances and the sheer amount of data now available about billions of *other* people, discretion no longer suffices to protect your privacy.”<sup>72</sup> Even if you have comprehensively avoided all social media and taken all recommended actions to protect your digital tracks, Facebook and other less visible enterprises that track across the web (i.e. not just through their own services) create “shadow profiles” to track the web actions of non-users.<sup>73</sup> Thus, through the actions of millions of others, the faces and actions of even non-participants are tracked.

The opt-in versus opt-out issue is but one small illustrative example of much broader challenges. A rebalancing is critically needed between the currently subjugated rights and freedoms of human beings against the overly emphasized rights and freedoms of commercial data gathers and processors.<sup>74</sup>

After gaining “personhood” through Supreme Court interpretations, the rights of corporations under the Bill of Rights have persistently been held to override competing Constitutional privacy rights for individual humans.<sup>75</sup> The Court has been increasingly willing to substitute its own will

---

privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/, last accessed 13 Feb 2020. Further, applying “well-established linguistic readability tests to the 500 most popular websites in the U.S. that use sign-in-wrap agreements,” researchers in 2019 found that “the average readability level of these agreements to be comparable to the usual score of articles in academic journals, which typically do not target the general public.” U. Benoliel and S. Becher, ‘The Duty to Read the Unreadable,’ *Boston College Law Review* 60: 2255 (2019), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3313837](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3313837)

<sup>72</sup> Z. Tufekci, ‘Think You’re Discreet Online? Think Again’, *New York Times* (April 21, 2019).

<sup>73</sup> L. Gowans, ‘Facebook Shadow Profiles: A Profile of You That You Never Created’, *Spider Oak* (2015), <https://medium.com/@SpiderOak/facebook-shadow-profiles-a-profile-of-you-that-you-never-created-302f99f20930>, last accessed 23 May 2019.

<sup>74</sup> Tomain, ‘Online Privacy and the First Amendment’, 70.

<sup>75</sup> There has never been a “corporate rights” movement by the U.S. public. Rather, the civil rights of corporations have been acquired through the courts. The U.S. Supreme Court decided the first constitutional rights case for corporations in 1809. The Fourteenth Amendment was drafted and then ratified in 1868 to “guarantee the rights of the freed slaves, not to protect corporations.” (Winkler, *We The Corporations*, xiii) Yet, it “has been transformed into a sword used by corporations to strike at unwanted regulation.” (xv). “Between 1868, when the amendment was ratified, and 1912, when a legal scholar set out to identify every Fourteenth Amendment case heard by the Supreme Court, the justices decided 28 cases dealing with the rights of African Americans – and an astonishing 312

and judgement for that of legislative bodies.<sup>76</sup> Congress and State legislatures as a result are very limited in their ability to mandate that businesses provide means for users to efficiently and regularly change privacy exposure settings in their use of web services.

Legislative bodies are also very limited under current interpretations of the Constitution in their ability to force human user consent or even user knowledge of the sale, licensing, trading, exchange, and mining of data that has been gathered from humans and their actions. Whether data is gathered from users from across the web, from mobile devices, or in their direct interactions with corporations, other businesses, and government, users should always assume that the data will be saved, processed, and that algorithmic mining will affect future individualized opportunities for each of us.

It is unlikely that the U.S. Supreme Court will change course in its stance on personhood for corporations after so many decades have passed under a counter interpretation to that of Professor Black's. The most likely means of changing the law at its foundations would be through a *human rights* amendment to the U.S. Constitution that would make it clear that the rights of individual humans should be preeminent over corporate rights when in direct conflict. In the event that economic inequality continues to expand and societal disruptions become severe, persistent, and widespread across the nation, passage of such an amendment may prove to be achievable at some point in the future though it seems unlikely at present.

***Human Ownership of Private Personal Information:*** During the 1960's and 1970's, well before the emergence of the internet, the law was largely mute concerning constraints that might be imposed on the private sector and government in the gathering and use of personal information about individuals. Gathering, exchanging, and selling facts about individuals without their knowledge or consent by the commercial sector expanded rapidly. The law seemingly provided no viable protection within the realms of either intellectual property law or privacy law. The weight of First Amendment law as it had developed over time favored an unregulated and unrestricted marketplace in information and personhood for corporations. This enabled corporations to gain the economic benefits of personal data with little to no consideration for the competing interests of the human beings who are the data subjects.

In 1967, Alan F. Westin, Professor of Public Law and Government at Columbia University, published *Privacy and Freedom*<sup>77</sup> which established an influential discussion and principle framework for the development of U.S. privacy law over the next couple of decades. He defined privacy as "the ability to determine for ourselves when, how, and to what extent information about us is communicated to others." Citizen protection provisions comports with this definition, for example, were incorporated into the Privacy Act of 1974.<sup>78</sup> This was the first law to impose controls on the collection, maintenance, use and dissemination of information about individuals by federal government agencies. The same controls were not generally imposed by law on the commercial sector.

---

cases dealing with the rights of corporations." (xv). Even though never subjected to systematic oppression, corporations as well have gained substantial protections through application of the Fourteenth Amendment and further Constitutional personhood rights.

<sup>76</sup> Tomain, 'Online Privacy and the First Amendment', 70.

<sup>77</sup> A. Westin, *Privacy and Freedom* (New York, 1967).

<sup>78</sup> Privacy Act of 1974, 5 U.S.C. § 552a

In his work, Professor Westin sought to see “personal information defined in terms of property rights so that the information couldn’t be “taken” without due process.”<sup>79</sup> Westin argued that “personal information, thought of the right of decisions over one’s private personality, should be defined as a property right with all the restraints on interference by public or private authorities and due process guarantees that our law of property has been so skillful in devising.”<sup>80</sup> Two years after Westin’s book, Arthur Miller picked up on the idea and suggested: “Perhaps the most facile approach to safeguarding privacy is the suggestion that control over personal information be considered a property right vested in the subject of the data and eligible for the full range of constitutional and legal protection that attach to property.”<sup>81</sup>

Westin as well hoped for the future development of a constitutionally protected general right of privacy. He did not see the need for a federal constitutional amendment to achieve this goal of protecting personal privacy through a property right since the constitution already provided the basis on which such a general right could be developed by the courts. This has yet to transpire.

Twenty-five years after Westin’s canonical book, Anne Wells Branscomb published a book titled *Who Owns Information?: From Privacy To Public Access*.<sup>82</sup> Anne Wells Branscomb was a communications and computer lawyer, held guest faculty positions at Yale, Columbia, and Tufts Universities, and was affiliated with the Harvard University Program on Information Resources Policy.<sup>83</sup> Among other insights, she reintroduced to the legal scholarly community the idea that private personal information such as “our names, addresses, and personal transactions are valuable information assets” in which each of us should have property rights.<sup>84</sup> With such a property right, data might be legally controlled primarily by each human that created the information through their actions even though not recorded in a tangible medium directly by the human subject. That is, certain personal data should not be controlled and distributed by any other person or entity that might happen to be in a position to be able to collect or acquire that information or data.

One might envision a *sui generis* right in certain personal data granted by society to humans similar to copyright. In order to provide reasonable access and use by the public, an author or artist’s copyright is not absolute. It is proscribed by such concepts as applying to only those works as defined within the wording of the copyright act, does not apply when no copying has taken place (e.g the act of reading a book is not a violation), and the author’s rights are limited by such legal concepts as fair use and the First Sale doctrine.

In a similar manner, humans might be granted strong control over copying of the data they create through their day-to-day actions in the world (often placed in a tangible form currently by electronic devices over which they have little to no practical control) but with the granting of

---

<sup>79</sup> O.M. Reynolds, Jr., ‘Review of Privacy and Freedom’, *Administrative Law Review*, 22:1 (October 1969), 101-106.

<sup>80</sup> Westin, *Privacy and Freedom*, 324-325

<sup>81</sup> A. R. Miller, ‘Personal Privacy in the Computer Age: The Challenge of New Technology in an Information-oriented Society’, *Michigan Law Review*, 67 (April 1969), 1224-1225.

<sup>82</sup> A. W. Branscomb, *Who Owns Information: From Privacy to Public Access* (New York, 1994). Recall that the first website went live in 1991, during the writing of this book in 1993 only 130 online websites existed in the world, and in 1995 the original NSFNET backbone was decommissioned as the Internet was transformed to a commercial enterprise. (See <https://www.businessinsider.com/flashback-this-is-what-the-first-website-ever-looked-like-2011-6>, <https://www.internetlivestats.com/total-number-of-websites/>, and <https://www.livescience.com/20727-internet-history.html>)

<sup>83</sup> ANNE WELLS BRANSCOMB, <http://www.branscomb.org/anne.html>, last accessed 23 May 2019

<sup>84</sup> Branscomb, *Who Owns Information*, 29

reasonable access to others in society with whom they interact. As with a copyrighted book, others would not be able to copy the private personal material and pass it on without the explicit permission of the human possessing the *sui generis* right. In this manner, individual humans would have much greater control over the conditions under which their private data is made available to others and would allow them, if they desired, to generate direct income from data aggregators.

At the time Branscomb proposed imposing personal property concepts as a means to protect individual privacy, some privacy advocates severely criticized the approach arguing that personal data should never be up for sale by anyone but should instead be protected primarily by legislation as a fundamental human right. Legislation defining a universal human right providing personal privacy protection, however, was never forthcoming. Nor was a human rights body of law developed through constitutional interpretation that could have appropriately dampened corporate rights.

At the time of Westin's book as well as twenty-five years later during Branscomb's writings, it was difficult to envision how such a property rights regime might be supported technologically. With recent advancements in networking and secure online monetary transfers, that is no longer the case.

Under the Westin/Branscomb paradigm one might now envision the emergence of a competitive network of brokers that would represent individual human beings, determine their desires in terms of limits on the use of their personal data (e.g. which private data, for what purpose, and for how long), and then negotiate prices and conditions with corporations and other entities desiring access. In this manner citizens would be legally enabled to take control over their own information privacy and choose exposure options ranging from tight control over their privacy to experimentation with minimal constraints allowing them to choose to maximize revenue streams from the use of their personal data. Currently, of course, such data is used with no direct financial income to the human data subjects.

Jaron Lanier, often credited as a founding father of Virtual Reality<sup>85</sup>, argues that "there is more than one way to build an information economy, and we have chosen the self-destructive path."<sup>86</sup> He expands upon several of the concepts articulated earlier by Westin and Branscomb.

Under a more humanistic information economy, Lanier envisions that individual humans would be the bearers of economic rights in information pertaining to themselves or which they produce through their existence or efforts rather than the primary bearers of such rights being the providers of information, services, and products. He envisions a world in which each human would have a negotiated relationship with each dominant server with which that individual interacts. It would be illegal to record information about more than one hundred individuals on the basis of click-through-licenses without negotiation for financial compensation to the people whose data is stored. He envisions a digital economy emerging in which hundreds of millions of people would be engaged in a universal system of micropayments. A user would typically sell to

---

<sup>85</sup> N. Firth, 'Virtual reality: Meet founding father Jaron Lanier', *New Scientist* (19 June 2013), <https://www.newscientist.com/article/mg21829226-000-virtual-reality-meet-founding-father-jaron-lanier/>, last accessed 23 May 2019.

<sup>86</sup> J. Lanier, *Who Owns the Future?* (New York, 2013), 360

the systems with which they interact as well as buy from them. Intermediary brokers would likely emerge to negotiate data fees for most humans.<sup>87</sup>

Brokers might compete for human clients and would market their clients' data to the services desired by each client. Each human client could set their own contractual conditions, typically through a check list process with a broker, addressing such issues as what data, for how long, at what price, for what purposes, and other conditions such as contractual damages and means for resolving disputes.

One may argue that very little money on average would actually accrue to the hundreds of millions of humans who might choose to participate in giving up certain of their personal information property rights in exchange for fees or royalties.<sup>88</sup> If true, such an approach would do little to correct the trend toward escalating economic inequality between data subjects and those with wealth concentration resulting from the free use of personal data.

On the counter side, one might envision rapidly growing numbers of search engines, social networking, and marketplace services competing with each other to acquire personal data rights from humans creating a vibrant and growing marketplace in such services. One might also envision the development of information infrastructure options that would use no personal information property in order to avoid the large overhead to protect such rights. With property rights in critical classes of personal data, individual humans would have an effective means to completely "opt out" from widespread data mining if desired since class action law suits from those who had property rights ignored would become a realistic possibility. The growth of competition among online search engines, social networking, and marketplace services as a result of differentiated personal information property interests by millions of humans as opposed to the current dominance of "siren servers"<sup>89</sup> using personal data for free might have the greatest effect on reducing economic inequality in society.

There is little doubt that conversion to a property rights regime for personal data is rife with challenges and would cause substantial disarray in the current information industry. However, if economic inequality continues to expand and societal disruptions become sufficiently severe, persistent, and widespread, public opinion may sway to the point where such an approach would be far more palatable to Congress and the courts.

---

<sup>87</sup> Lanier and Well envision the emergence of "mediators of individual data" (MIDS) that might be organized as non-profit or business groups adhering to eight core principles with humans joining multiple groups. See J. Lanier and E. G. Well, 'A Blueprint for a Better Digital Society', *Harvard Business Review* (26 Sept 2018).

<sup>88</sup> See E. Chivot, *Paying Users for Their Data Would Exacerbate Digital Inequality*, (11 Jan 2019), <https://www.datainnovation.org/2019/01/paying-users-for-their-data-would-exacerbate-digital-inequality/>, last accessed 23 May 2019 and L. Schafer, 'How much are your online data really worth?', *Star Tribune* (Minneapolis), (12 April 2018), <https://phys.org/news/2018-04-online-worth.html>, last accessed 23 May 2019. A partial counter stance is described by L. Hautala, *California wants Silicon Valley to pay you a data dividend: The Golden State thinks tech companies should share the wealth*, (25 Feb 2019), <https://www.cnet.com/news/california-wants-silicon-valley-to-pay-you-a-data-dividend/>, last accessed 23 May 2019. A formal analytical model for assessing the value of data (D) supplied by human users versus the value of utility (U) received from the information services has been proposed by Noam Kolt (i.e. Return on Data (ROD) = U/D). See N. Kolt, 'Return on Data', 38 *Yale Law & Policy Review* (forthcoming 2019).

<sup>89</sup> Lanier, *Who Owns the Future?* 53-58.

## 9. CONCLUSION

The effects of pervasive tracking and algorithmic controls, while providing many benefits, have also resulted in numerous and substantial negative effects on both individuals and on society as a whole. A range of short to long-term solutions have been suggested in the literature and by legislators for lessening or eliminating the most egregious of the adverse consequences. The authors suggest that, rather than addressing challenges piecemeal, the time is appropriate to reexamine legal foundation readjustments that might lead to vibrant information economies that as well support and respect the agency and autonomy of individual humans.

Under the current U.S. legal paradigm, large amounts of data are amassed from hundreds of thousands of businesses, web applications, financial institutions, and governments. This data is exchanged among businesses to provide access to each other and additional businesses, extensively mined, and put to purposes that benefit primarily the involved businesses without engaging the humans whose actions in living have generated the data.

Long hypothesized threats to the autonomy of humans to think and decide for themselves<sup>90</sup> are now being realized on a widespread basis under the pervasive tracking regimes supported by U.S. law. The approaches considered in this study provide some paths to consider as social and economic disparities may grow to the point of creating political crises in this age of expanding pervasive tracking and algorithmic controls. Reconsideration of Professor Black's constitutional reasoning in support of *human rights* as well as Alan Westin's and Anne Branscomb's ideas advocating for *human ownership of private data* might yet have great efficacy in rebalancing the rights of humans as against those of corporations in the handling of private personal data. Both of these approaches could also provide a fundamental framework for the future balancing of human versus business and government interests in the ever expanding uses of pervasive location, place, and transaction data tracking. These ideas also have substantial potential for guiding ethically defensible and legal uses for future applications of AI, autonomous machines, and robots. For long term solutions, we need to get back to basics in correcting our political, legal and economic foundations.

---

<sup>90</sup> Project on Computer Databanks, National Academy of Sciences, *Databanks in a Free Society: Computers, Record-Keeping, and Privacy* (Washington D.C. 1972)