BEING HUMAN IN AN ALGORITHMICALLY CONTROLLED WORLD

HARLAN ONSRUD AND JAMES CAMPBELL

Abstract *Most people in developed countries, and many in developing countries, 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.*[1] *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.*[2] *Those criteria almost always involve location-based and place-based data. In this paper, we consider effects of those computational tools on individual choice and autonomy and on societal structure from the humanistic perspectives of philosophy and jurisprudence. Specifically, we:*

- *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.*

Keywords: personal information privacy, location-based data, location privacy, economic inequality, surveillance capitalism, human rights

International Journal of Humanities and Arts Computing 14.1-2 (2020): 235–252
DOI: 10.3366/ijhac.2020.0254

www.euppublishing.com/ijhac

1. INTRODUCTION

The advent of computationally based modern information systems has changed the nature of commerce and of society in developed economies. Those changes have provided significant benefits in many aspects of daily life, often based on location-based data, e.g., driving directions via GPS. The intersection of location-based analysis with traditional scholarly studies in many fields of the humanities has proved fertile for understanding human experience in both contemporary and historical contexts.[3] Part of understanding human experience today involves understanding the effects that our advanced information systems, and particularly location-based and place-based systems, can have on human beings as philosophically autonomous agents.

Understanding of the tracking of human beings today needs to transcend the traditional bounds of the geohumanities and spatial humanities. Inclusion of knowledge from jurisprudence, philosophy, and other humanistic disciplinary domains is essential if the geospatial humanities are to contribute at a foundational level to addressing location data gathering and processing challenges.

In this paper, we examine some of the negative effects of these systems on human autonomy and agency, and suggest some possible approaches from a jurisprudence perspective to moderate those negative impacts on individuals and on societies.

Modern information systems gather detailed location-based, place-based, and transactional data that is aggregated, accessed, exchanged, and sold among businesses[4] 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 of beneficence, non-malfeasance, justice, and individual autonomy.[5] Most commercial information systems incorporating big data are blind to such considerations.[6] 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 an 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. Facebook, for example, has filed a patent on a process to predict a person's future location.[7] This allows them to predict when a person will be in locations without internet access allowing them to preload ads and other information on that person's device to make it still accessible without network access. Similarly, Google Maps for Android announced its 'Driving Mode' feature in 2016 which guessed a driver's destination based on location history and web search behavior. The backlash caused Google not to modify the practice but to make the calculated destinations merely 'suggestions.'[8]

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 make informed decisions in their own interests, 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 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 which are, for most people, intertwined with economic adequacy and well being. 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.'[9] 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 tripled, and that of the top .001 percent has risen more than sevenfold'.[10] 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.[11] 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.[12] Only 50% of Americans born in the 1980s can expect to earn more than their parents.[13]

To date, 'Half the decline in workers' share of income in the developed world can be attributed to advancing technology.'[14] In many fields, technology is substituting for labor.[15] This reality is having dramatic consequences for middleclass jobs.[16] 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.[17,18]

The current problem in the US 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.[19] Job prospects for these individuals will continue to worsen without substantial societal realignments.

The legal system in the US 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.[20] 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.'[21]

Amazon has created a commerce infrastructure capturing 'nearly $1 out of every $2 that Americans spend online' thereby dwarfing the breadth, depth, and size of monopolistic financial empires that were disbanded in previous times under US law.[22]

Large companies able to attract very large user bases with continually updated 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 and 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.

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 alone 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 desired link when a different word, phrase 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. This type of automated testing is repeated thousands of times per day by most dominant online enterprises. 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.

While the machine-derived algorithms arising from the mining of massive data collections have already been highly 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.

Documented examples include automated discrimination against women in executive searches, rejection of identification of dark-complexioned parties through facial recognition software, discrimination against people seeking room reservations with distinctly sounding African-American names, 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. Guilt-by-association profiling almost always incorporates location-based data. In the future, machines will additionally estimate our emotions using biometric measures as we view information or

images on screens as further input into assessing suitability for product offerings, or susceptibility to social decisions up to and including voting in elections.[23]

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.[24] How to deploy and enforce such capabilities is not clear although efforts are beginning to attempt to better understand these processes.[25]

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.[26] 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, and conducting surgery. No current employment sector will be untouched. Forty-seven percent of US workers have a high probability of having their jobs automated over the next 20 years.[27]

'The inability of the US economic and political system to address basic problems angers ordinary citizens and intensifies mistrust in democratic institutions.'[28] If the US 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.'[29]

4. 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 . . .[30]

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.'[31] 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.[32]

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.'[33] Corrective laws and jurisprudence are still possible. New forms of ownership and methods of production may be created.

5. SUGGESTED SOLUTIONS

On an economic level, a fundamental research question for our algorithmic era is how information societies can enable 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 the 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 jobs,
- widespread implementation of paid family and parental leave,
- universal health care,
- remunerating work such as parenting, volunteering, and mentoring,

- expansion of the earned income tax credit,
- 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.[34]

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.[35]

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 US in the future as income inequality and societal disruptions become more pronounced.

Economic livelihood is critically important to human existence, entwined as it is with human 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. Examples include 'privacy by design' and bringing short-term technical expertise to bear in the formulation of corporate practice and the creation of legislation.[36] Privacy considerations could thereby become stronger priorities within legislative and corporate initiatives that effect human autonomy and agency through data collection and processing.

6. LEGAL FOUNDATIONAL ADJUSTMENTS

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

- legislation or constitutional reforms that would far better enable control by individuals over their personal information exposure,
- substantive campaign finance reform which, as a prerequisite, would require a constitutional amendment to overturn Citizens United v. Federal Election Commission, 558 US 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,
- 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 chapter is focused.

7. REVISITING HUMANISTIC INFORMATION ECONOMIC AND LEGAL APPROACHES

The core of this work considers innovative reforms offered by leading legal scholars when the Internet and information economy were nascent. 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.

Major advancements in technology make these approaches much more achievable today than when initially proposed, and 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.

A New Birth for Human Rights:

Professor Charles L. Black, Jr. over his thirty-one-year career at Yale 'made Yale Law School one of the world's leading centers for the study of constitutional law.'[37] When in his eighties, he reemerged from retirement in 1997 to write a short book 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'[38] and then sets forth meticulously '… the construction of a better system of reason for the grounding of constitutional human rights in this country.'[39]

He critiques the judicial reasoning of past Supreme Courts in misinterpreting the nation's founding documents in extending the Bill of Rights (eight of the first ten amendments) to corporations. 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 US 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 Fourth Amendment (*as those clauses ought to have been and still ought to be interpreted.*)' (Emphasis added)[40]

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.' '[41]

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 US 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.[42] 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 US Supreme Court would not uphold legislation requiring an opt-in approach for data mining commercial activities but would instead continue to expand protection for commercial free speech.[43]

Absent government regulation, 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.

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.

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.'[44] Even if an individual has comprehensively avoided all social media and taken all recommended actions to protect his or her 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.[45] 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.[46]

Legislative bodies are very limited under current interpretations of the Constitution in their ability to force 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 algorithmic mining will affect future individualized opportunities for each of us.

It is unlikely that the US 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 US 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 privacy law or intellectual property 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*[47] which established an influential framework for development of US 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 comporting with this definition, for example, were incorporated into the Privacy Act of 1974.[48] 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.

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.'[49] Westin argued that 'personal information, thought of as 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.'[50] 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.'[51]

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*.[52] 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.[53] With such a property right, data might be legally controlled primarily by each human that created the information through their actions, even though recorded in a tangible medium by or for the human subject through carried or stationary electronic devices. 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 but with the granting of 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.

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[54], argues that 'there is more than one way to build an information economy, and we have chosen the self-destructive path.'[55] 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 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 the systems with which they interact as well as buy from them. Intermediary brokers would likely emerge to negotiate data fees for most humans.[56]

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 though 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 chose to participate in giving up certain of their personal information property rights in exchange for fees or royalties.[57] 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.

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.

8. 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 also support and respect the agency and autonomy of individual humans.

Under the current US legal paradigm, large amounts of data are collected by 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 primarily benefit 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[58] are now being realized on a widespread basis under the pervasive tracking regimes supported by US 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.

END NOTES

[1] H. Fry, *Hello World: Being Human in the Age of Algorithms* (New York, 2018), 3.

[2] D. M. West, *The Future of Work: Robots, AI, and Automation* (Washington D.C., 2018), 64–79.

[3] In this paper, we use the definition of Humanities used by the National Endowment for the Humanities. See https://www.neh.gov/information-first-time-applicants

[4] By example, more than 1,000 apps contain location-sharing code. Sales of location-targeted advertising alone was estimated at $21 billion in 2018. J. Valentino-DeVries, N. Singer, M. Keller and A. Krolik, 'Your Apps Know Where You Were Last Night,

and They're Not Keeping It Secret,' *New York Times* (10 Dec 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

[5] T. Beauchamp and J. Childress, *Principles of Biomedical Ethics,* 6th ed. (Oxford, 2008).

[6] 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.

[7] N. Nguyen, 'Facebook Filed A Patent To Calculate Your Future Location', *Buzzfeed* (10 Dec 2018), https://www.buzzfeednews.com/article/nicolenguyen/facebook-location-data-prediction-patent

[8] Nguyen, 'Facebook Filed A Patent To Calculate Your Future Location'.

[9] A. Giridharadas, *Winners Take All: The Elite Charade of Changing the World* (New York, 2018), 5.

[10] Giridharadas, *Winners Take All,* 4, 16.

[11] Giridharadas, *Winners Take All,* 16.

[12] Giridharadas, *Winners Take All,* 4.

[13] West, *The Future of Work,* 138.

[14] M. Schuman, 'Why Wages Aren't Growing', *Bloomberg Businessweek*, (25 Sept 2017).

[15] West, *The Future of Work,* 67.

[16] West, *The Future of Work,* 67–68, 153.

[17] D. Rotman, 'Who Will Own the Robots', MIT Technology Review (Sept 2015).

[18] M. Muro, S. Liu, J. Whiton, and S. Kulkarni, 'Digitalization and the American Workforce,' Metropolitan Policy Program, Brookings Institution (Nov 2017).

[19] West, *The Future of Work,* 66, 79, 81, 108.

[20] Giridharadas, *Winners Take All,* 5.

[21] E. Brynjolfsson and A. McAfee, The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies (New York, 2014), 172.

[22] Mitchell**,** **'**Amazon Doesn't Just Want to Dominate the Market', The Nation, (15 Feb 2018), 5.

[23] West, *The Future of Work*, 35–39.

[24] C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York, 2016), 231.

[25] See e.g. R. Gordon, 'Building AI systems that make fair decisions', *MIT News* (April 24, 2018).

[26] West, *The Future of Work,* 68.

[27] West, *The Future of Work,* 70.

[28] West, *The Future of Work,* 138.

[29] A. Smith and J. Anderson, 'AI, Robotics, and the Future of Jobs', Pew Research Center (6 Aug 2014), 5.

[30] Zuboff, *The Age of Surveillance Capitalism*, 8.

[31] Zuboff, *The Age of Surveillance Capitalism*, 8.

[32] Zuboff, *The Age of Surveillance Capitalism*, 11.

[33] Zuboff, *The Age of Surveillance Capitalism*, 521.

[34] West, *The Future of Work,* 89–102.

[35] West, *The Future of Work,* 102–108.

[36] See, for example, 32nd Annual Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy by Design* (Jerusalem, 2010).

[37] Wikipedia, *Charles Black (professor)*, https://en.wikipedia.org/wiki/Charles_Black_(professor), last accessed 23 May 2019.

[38] Black, Charles L., Jr., *A New Birth of Freedom: Human Rights, Named and Unnamed*, (New York, 1997), 1.

[39] Black, *A New Birth of Freedom,* 4.

[40] Black, *A New Birth of Freedom, ix*.

[41] Black, *A New Birth of Freedom,* 38.

[42] US 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 in support of imposition of opt-in requirements, 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.

[43] Tomain, 'Online Privacy and the First Amendment', 63–64.

[44] Z. Tufekci, 'Think You're Discreet Online? Think Again', *New York Times* (April 21, 2019).

[45] 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.

[46] Tomain, 'Online Privacy and the First Amendment', 70.

[47] A. Westin, *Privacy and Freedom* (New York, 1967).

[48] Privacy Act of 1974, 5 USC. § 552a.

[49] O.M. Reynolds, Jr., 'Review of Privacy and Freedom', *Administrative Law Review*, 22:1 (October 1969), 101–106.

[50] Westin, *Privacy and Freedom*, 324–325.

[51] 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.

[52] A. W. Branscomb, *Who Owns Information: From Privacy to Public Access* (New York, 1994).

[53] Branscomb, *Who Owns Information*, 29.

[54] N. Firth, 'Virtual reality: Meet founding father Jaron Lanier', *New Scientist* (19 June 2013).

[55] J. Lanier, *Who Owns the Future?* (New York, 2013), 360.

[56] 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).

[57] 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). 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.

[58] Project on Computer Databanks, National Academy of Sciences, *Databanks in a Free Society: Computers, Record-Keeping, and Privacy* (Washington D.C. 1972).