LINCOLN MEMORIAL UNIVERSITY
LAW REVIEW

VOLUME 9 SUMMER 2022 ISSUE 3

THE INTERNET-OF-BODIES/HUMAN MIND UNIFICATION:

ITS THREAT TO DEMOCRACY AND THE NEED FOR A LEGAL RESPONSE

Zachary Atchley[*]

I. INTRODUCTION

This paper is intended to serve as a canary in the coal mine concerning the grave threat the Internet of Bodies poses to personal autonomy and democratic governance, as well as provide a consolidated snapshot of needed private market and legal responses. The ubiquity of the Internet, Artificial Intelligence (AI), the Internet of Things (IoT), and the Internet of Bodies (IoB) has brought with it unprecedented pro-social

[*]Zachary Atchley is a Third Year, 2022 JD Candidate at Lincoln Memorial University's Duncan School of Law. Atchley holds a Master of Public Administration from the University of Tennessee at Chattanooga and brings over a decade of experience in Nonprofit Administration to his burgeoning legal career. The author wishes to express his gratitude to Professor Sydney Beckman of Duncan School of Law for his guidance in writing this article and to his two daughters, Autumn and Aaralyn Atchley, for supporting their father in his new career aspirations.

technological capabilities, global connectivity, consumer convenience, and economic growth. However, it has also been radically disruptive psychologically, culturally, and politically in the lives of the individual and the collective. The current government and corporate inaction in the face of these negative forces carry a very real and serious existential threat to individuals' personal autonomy and decisional privacy, as well as to the practice of democracy itself.[1]

This threat is most pronounced with the growing emergence of the Internet of Bodies (IoB). The IoB is the growing "network of human bodies whose integrity and functionality rely at least in part on" connecting the Internet and AI to technologies affixed to the human body.[2] The IoB's ultimate and highest expression is the Brain Control Interface (BCI). BCIs are beginning to achieve the physical and informational unification of the human mind with the AI mind via direct bidirectional communication. Once fully realized, BCIs will provide unprecedented access and influence into democracy's most holy sanctuary—the individual's mind. This highlights the extraordinary psychological, political, and legal ramifications implicated by the IoB.

This IoB-human mind nexus will serve as the focal point of this analysis for three reasons. First, the IoB-human mind nexus is where law, technology, and an individual's personal autonomy and decisional privacy meet. Secondly, it dramatically illustrates technology's coming potential and the urgent privacy and security threats brought upon by technological advancements. And lastly, it illuminates the legal and practical constraints in mitigating these threats due to the patchwork of disparate legal responses meant to govern the complex structure and function of the global technological architecture underpinning information technologies, artificial intelligence, and the Internet.

Part I will define individual autonomy and decisional privacy, highlighting its centrality to democracy. Part II

---

[1] Carlos I. Gutierrez, *Can Existing Laws Cope with the AI Revolution?*, BROOKINGS (Nov. 12, 2021, 8:53 PM), https://www.brookings.edu/techstream/can-existing-laws-cope-with-the-ai-revolution/.

[2] Andrea M. Matwyshyn, *The Internet of Bodies*, 61 WM. & MARY L. REV. 77, 77 (2019).

presents a science-based, info-centric view of humans as information processing algorithms. Ideas from physics, biology, and cognitive science are used to detail the technical reality of the IoB-human mind unification and its profound connection to autonomy and decisional privacy. Next, Part III explains how humans act as information processing algorithms and how the IoB-human mind nexus is made possible through Internet-connected sensors, actuators, and the process of transduction. Specifically, transduction converts one form of energy/information into another form of energy/information.[3] Part III concludes with an introduction to the Internet-of-Bodies and a survey of IoB products.

To highlight the imminent privacy and security threats that the coming IoB-human mind unification brings to personal autonomy and democracy, Part IV situates it within two global trends—one political and one psychological. The political trend concerns the recent rise in authoritarianism and a corresponding decline in global democracy.[4] The psychological trend concerns what historian and thought leader Yuval Harari calls the twenty-first century's New Human Agenda—the quest to attain immortality, happiness, and super-human abilities through bio- and info-technologies.[5] Part IV concludes by detailing how current, non-IoB technologies erode individual autonomy and catalyze the decline in democracy, thus foreshadowing IoB's effect.

Part V responds to all these concerns by offering a comprehensive snapshot of pragmatic and principled responses for governing the IoB, focusing on securing its most vulnerable transduction node, the IoB-human mind nexus. The snapshot highlights the work of Andrea Matwyshyn and Laura Denardis. For example, Matwyshyn argues that safeguarding personal autonomy and decisional privacy should be the

---

[3] LAURA DENARDIS, THE INTERNET IN EVERYTHING: FREEDOM AND SEC. IN A WORLD WITH NO OFF SWITCH 46 (Yale Univ. Press 2020).

[4] *Global Democracy has a Very Bad Year: The Pandemic Caused an Unprecedented Rollback of Democratic Freedoms in 2020*, THE ECONOMIST, https://www.economist.com/graphic-detail/2021/02/02/global-democracy-has-a-very-bad-year (last visited Nov. 12, 2021).

[5] YUVAL N. HARARI, HOMO DEUS: A BRIEF HISTORY OF TOMORROW 21 (Harper Perennial 2017).

central, permeating legal principle governing the IoB.[6] Laura Denardis' supremely pragmatic approach focuses action on the five "[l]evers of control in Internet governance."[7] Building from this core framework, Part V concludes with a survey and assessment of federal and state data privacy and security laws, as well as other proposed legal remedies.

II. PART I: PERSONAL AUTONOMY, DECISIONAL PRIVACY, AND DEMOCRACY.

According to the United States Supreme Court, "[l]iberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct."[8] Democracy, in turn, presumes personal autonomy as a "fundamental political value" because the legitimacy of a democratic government "depends upon the rational consent of its citizens."[9]

At its core, personal autonomy equates to a self-governing agency.[10] This self-governance applies to an individual's thoughts and actions and relies on certain psychological and social preconditions.[11] Autonomy's psychological preconditions relate to mental competencies and authentic personal identities.[12] Mental competencies required for self-rule include "rational thought, self-control, [as well as] freedom from debilitating pathologies [and] systemic self-

---

[6] Matwyshyn, *supra* note 2, at 164.
[7] DENARDIS, *supra* note 3, at 18-19.
[8] Lawrence v. Texas, 539 U.S. 558, 562 (2003).
[9] Michael Pendlebury, *Individual Autonomy and Global Democracy*, 103 THEORIA: A JOURNAL OF SOCIAL AND POLITICAL THEORY 43, 45 (Apr. 2004).
[10] Sarah Buss & Andrea Westlund, *Personal Autonomy*, THE STAN. ENCYCLOPEDIA OF PHIL. (Feb. 15, 2018), https://plato.stanford.edu/archives/spr2018/entries/personal-autonomy/.
[11] Andrew J. Boyd, *Medical Marijuana and Personal Autonomy*, 37 J. MARSHALL L. REV. 1253, 1279 (2004).
[12] John Christman, *Autonomy in Moral and Political Philosophy*, THE STAN. ENCYCLOPEDIA OF PHIL. (June. 29, 2020), https://plato.stanford.edu/archives/fall2020/entries/autonomy-moral/.

deception."[13] Authenticity places these competencies in the service of one's identity. An authentic individual self-reflexively evaluates her motives and actions against her existing beliefs, values, and goals, and she adjusts and/or acts upon each accordingly.[14] Individual autonomy's social preconditions include the availability of meaningful choices[15] and the "independence of one's deliberation and choice from manipulation by others."[16] Notably, meaningful independent choices depend on "decisional privacy"[17] and "freedom from monitoring, scrutiny, interference, and categorization by others."[18] The Supreme Court, in *McIntyre v. Ohio Elections Commission*, stated that – "[a]nonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose behind the Bill of Rights, and the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society."[19]

Democratic political theory and governance depend upon personal autonomy as both a virtue and a right. In his seminal work, *A Theory of Justice*, the preeminent political philosopher, John Rawls, uses the ideal of an autonomous, unbiased, and rational decision-making agent as a first principle to formulate and justify all subsequent political principles and structures of a democratic social contract.[20] Likewise, political philosophers use this idealized agent "to delineate and critique oppressive social conditions, liberation from which is considered a fundamental goal" . . . because "being guided by forces external to the self and which one cannot authentically embrace . . . mark[s] the height of oppression."[21] To this end, the United States Constitution and judiciary have demarcated zones of privacy—protecting certain

---

[13] *Id.*

[14] Buss, *supra* note 10.

[15] Boyd, *supra* note 11, at 1281.

[16] Christman, *supra* note 12.

[17] Karl Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J. L. & TECH. 106, 131 (2019).

[18] Sofia Grafanaki, *Autonomy Challenges in the Age of Big Data*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 803, 809 (2017).

[19] McIntyre v. Ohio Elections Commission, 514 U.S. 334, 357 (1995).

[20] JOHN RAWLS, A THEORY OF JUSTICE (Harv. Univ. Press) (revised ed. (1999)).

[21] Christman, *supra* note 12.

fundamental rights—each being a corollary of "individual dignity and autonomy" and designed to shelter individuals' thoughts and actions from, what has historically been the most powerful source of coercion, the State.[22]

Information technologies are now threatening these sacrosanct zones of privacy in unprecedented and insidious ways, and legal protections of these zones are inadequate, anachronistic, and misguided, given the fact that private companies, motivated by market forces, increasingly control technology's reach into and influence on the human mind, not the State. However, before exploring technology's threats to autonomy and its challenges to democracy, it is vital to understand the science and architecture behind these technologies so that one can appreciate the Internet-of-Bodies imminence, grasp the urgency of needed action, and effectively tailor legal responses. As the secular prophet, Carl Sagan, foretold in 1995's *The Demon Haunted World: Science as a Candle in the Dark*,

> I have a foreboding of an America in my childrens' or grandchildrens' time – when the United States is a service and information economy; when nearly all the key manufacturing industries have slipped away to other countries; when awesome technological powers are in the hands of a very few, and no one representing the public interest can even grasp the issues; when the people have lost the ability to set their own agendas or knowledgeably question those in authority; when, clutching our crystals and nervously consulting our horoscopes, our critical faculties in decline, unable to distinguish between what feels good and what's true, we slide, almost without noticing, back into superstition and darkness.[23]

---

[22] Obergefell v. Hodges, 576 U.S. 644, 644 (2015); *see* also Griswold v. Connecticut, 381 U.S. 479 (1965).

[23] CARL SAGAN, DEMON-HAUNTED WORLD: SCIENCE AS A CANDLE IN THE DARK 25 (Balantine Books 1996).

III. PART II: AN INFO-CENTRIC VIEW OF HUMANS AS INFORMATION PROCESSING ALGORITHMS.

The Internet of Bodies-human mind connection is technologically possible because humans, just like information technologies, are fundamentally a bundle of information processing algorithms. This is not hyperbole; it is orthodox science. Two foundational concepts underlie this fact: (1) information is physical, and (2) all organisms operate as algorithms. This section will flesh out information theory and chart the course of algorithms from physics to evolution, from evolution to the human mind, and finally, from the human mind to the artificial intelligence embedded in today's information technologies. Part III will then illustrate how humans, as information processing algorithms, make the IoB-human mind nexus a practical reality.

A) INFORMATION IS PHYSICAL

The public mind considers information intangible, non-physical, and almost mystical. In reality, however, well-established physics has determined that "information is a physical phenomenon."[24] This is evidenced by information and energy's intimate connection and has been mathematically represented as an algorithm known as Landauer's Principle.[25] Landauer's Principle states that,

> Any logically irreversible manipulation of information, such as the erasure of a bit or the merging of two computation paths, must be accompanied by a corresponding entropy increase in non-information bearing degrees of freedom of the information processing apparatus or its environment.[26]

---

[24] LUCIANO FLORIDI, INFO: A VERY SHORT INTRODUCTION 60 (Oxford Univ. Press 2010).

[25] Charles H. Bennett, *Notes on Landauer's principle, reversible computation, and Maxwell's Demon*, 34 STUDIES IN HISTORY AND PHIL. OF MODERN PHYSICS 501 (2003).

[26] *Id.*

Caltech Physicist Sean Carroll stated the principle in more colloquial terms:

> We . . . write things down, all the time . . . [and] . . . lose our notebooks all the time, too. Landauer's Principle says there is a direct connection between these processes and the thermodynamic arrow of time, the increase in entropy throughout the universe. The information we possess is a precious, physical thing, and we are gradually losing it to the heat death of the cosmos under the irresistible pull of the Second Law [of Thermodynamics]. [27]

B) ORGANISMS ARE ALGORITHMS

Historian Yuval Harari says that "'[a]lgorithm' is arguably the single most important concept in our world," and that, "[i]f we want to understand our life and our future, we should make every effort to understand what an algorithm is, and how algorithms are connected to [human] emotions."[28] In simplest terms, an algorithm is a logically foolproof, step-by-step mechanical procedure that, if given certain inputs, will reliably produce a specific result.[29] These results can be calculations, decisions, actions, or things such as organisms or family meals because long division, computer programs, evolution by natural selection, and recipes are all algorithms.[30]

All algorithms share three necessary characteristics: (1) algorithms are substrate neutral, (2) algorithms are mindlessly mechanical, and (3) algorithms produce guaranteed results.[31] Algorithms are substrate neutral because of the nature of a symbol. A symbol is a piece of matter (i.e., a substrate) with a

---

[27] Sean Carroll, *Thanksgiving*, PREPOSTEROUS UNIVERSE (Nov. 12, 2021, 10:36 PM), https://www.preposterousuniverse.com/blog/2013/11/28/thanksgiving-8/.

[28] HARARI, *supra* note 5, at 83.

[29] DANIEL DENNETT, DARWIN'S DANGEROUS IDEA: EVOLUTION AND THE MEANINGS OF LIFE 50 (Simon & Schuster Paperbacks 1995).

[30] *Id*. at 51.

[31] DENNETT, *supra* note 29, at 50-51.

dual property—it "carries information, and it causes things to happen."[32] Numerical symbols illustrate this point. For example, addition and subtraction done by hand with pen and paper work just as well as addition and subtraction done by a computer using binary code in silicon. The mechanical mindlessness of an algorithm does not concern the complex design of the procedure or its elaborate results; rather, it speaks to the simple, cause-and-effect mechanical steps it takes without any foresight or knowledge in producing the outcome. Guaranteed results of algorithms concern the procedure's reliability—given certain inputs, the logical structure of the procedure will inevitably produce a certain outcome 100% of the time. These concepts will be explained by way of four causally connected examples: evolution by natural selection, genes, human bodies and brains, and artificially intelligent technologies.

C) Evolution by Natural Selection is an Algorithm

Modern biology has distilled the theory of evolution by natural selection into a simple lawful process, the algorithm of IF, IF, IF → THEN, which acts on the DNA molecule. The evolutionary algorithm is as follows: IF genetic variation exists, and IF genetic selection exists (i.e., non-random differential survival of genes due to limited resources and a struggle for life), and IF genetic heredity exists, THEN genetic evolution MUST occur.[33] In other words, evolution is best understood as information-based, substrate-neutral (because the same algorithm applies equally to RNA—DNA's predecessor), and mindless because the selection is mechanical environmental sifting.

D) The Genetic Code is an Algorithm

Genes are not only evolution's unit of selection; genes, too, are algorithms, and "genetics has become a branch of Information Technology."[34] Genes are digital information that

---

[32] Steven Pinker, How the Mind Works 66 (Norton Paperback 2009).
[33] Dennett, *supra* note 29, at 48-60.
[34] Richard Dawkins, A Devil's Chaplain: Reflections on Hope, Lies, Science, and Love 27-28 (First Mariner Books 2004).

behaves exactly like a software subroutine.[35] This genetic subroutine mindlessly and mechanically translates DNA into "the alphabet of amino acids which spell[] out protein molecules."[36] These protein molecules constitute the first step in a long, unbroken, algorithmic chain that ultimately results in a living organism. Richard Dawkins's observation in *The Selfish Gene*, that genes "are in you and in me; they created us, body and mind; and their preservation is the ultimate rationale for our existence"[37] provides the basis for the notion that humans are algorithms.

E) THE HUMAN ORGANISM—BODY AND MIND—IS AN ALGORITHM

The genetic code's algorithmic reach and informational nature extend to the highest realm of human identity—the human mind. Cognitive scientists and psychologists now view the mind as a network of specialized computation modules whose "basic logic is specified by" genetic coding.[38] Said differently, "[t]he mind is what the brain does . . . the brain processes information and thinking is a kind of computation."[39] This mindless computation results in human intelligence, "the ability to attain goals in the face of obstacles by means of decisions based on rational rules [(i.e., algorithms)]."[40]

What the computational theory of mind says about thoughts, emotions, beliefs, and desires is the most important consequence of understanding the Internet-of-Bodies. The computational theory of mind says that "beliefs and desires are *information* incarnated as configurations of symbols . . . [thus] planting them squarely *in the physical universe* . . . [and] . . . allow[ing] *meaning* to cause and be caused."[41] What we

---

[35] *Id*. at 28.
[36] RICHARD DAWKINS, THE SELFISH GENE 23 (Oxford Univ. Press 30th ed. 2006).
[37] *Id.* at 20.
[38] PINKER, *supra* note 32, at 21.
[39] *Id.*
[40] *Id.* at 62.
[41] PINKER, *supra* note 32, at 25.

experience as "sensations, emotions, and thoughts" are the operation of biochemical algorithms.[42]

F) ARTIFICIAL INTELLIGENT TECHNOLOGIES ARE ALGORITHMS

Artificial intelligent technologies are called such because they "emulate[] human cognition."[43] Artificial intelligent technologies only differ from human computational intelligence in substrate (silicon chips vs. carbon-based neurons), code (DNA/biochemical vs. binary code), and computing capacity (AI computation of big data far exceeds human computation). Artificial intelligence (AI) "relies on computer programs that can sense, reason, learn, act, and adapt" in similar ways to humans.[44] Likewise, more and more AI cyber-physical systems use these human-like skills autonomously, changing behavior and improving their decision-making completely independent of human intervention.[45]

Importantly, AI technologies possess two non-human abilities—connectivity and updatability.[46] It is probably more accurate to describe these abilities as super-human because it is connectivity and updatability that give AI technologies their unique power. Autonomous vehicles are exemplars. Researchers are developing connected vehicles via vehicle-to-vehicle communication technologies to reduce traffic accidents at intersections, which can also communicate with municipalities' artificially intelligent intersection management systems (such as traffic light systems). Therefore, when two autonomous vehicles approach the same intersection, they do not act as two separate entities but rather as a single algorithm. Additionally, if a municipality changes the speed limit or traffic light pattern, every autonomous car can be simultaneously

---

[42] HARARI, *supra* note 5, at 85.
[43] Manheim & Kaplan, *supra* note 17, at 113-14.
[44] *Id.* at 113.
[45] DENARDIS, *supra* note 3, at 48-49.
[46] YUVAL N. HARARI, 21 LESSONS FOR THE 21ST CENTURY 23 (Random House 2018).

updated with that information instantaneously.[47] Individual human drivers simply do not possess these powers of connectivity and updatability.

This deep exploration of information theory and the shared algorithmic nature of humans and artificially intelligent technologies, which makes the IoB-human mind connection possible, was intended to provoke the reader into a sense of discomfort because a consequence of the IoB is the practical hackability of meaning, sensations, emotions, and thoughts. The canary is dead in the coal mine.

The next section will explain transduction, the technical process that makes human and machine communication possible. Furthermore, it will introduce the Internet-of-Bodies (IoB), IoB products, and sketch the underlying global technological architecture of the IoB (AI and the Internet).

IV. PART III: TRANSDUCTION AND THE INTERNET-OF-BODIES

Given the shared nature of humans and AI technologies, a human is accurately conceptualized as an "interconnected informational organism . . . sharing with biological agents *and engineered art[i]facts*, a global . . . informational environment constituted by all informational processes, services, and entities."[48] Said another way, a human is a biochemical algorithm equivalent in kind *and connected to* artificially intelligent artifacts. This connection is made possible through a process known as transduction.

A. TRANSDUCTION – THE LINK BETWEEN HERE (ANALOGUE, CARBON-BASED, OFF-LINE) AND THERE (DIGITAL, SILICON-BASED, ONLINE).

Transduction is the conversion of one form of energy/information into another form of energy/information, such as electrical energy into mechanical energy.[49]

---

[47] RESA AZIMI ET AL, VEHICULAR NETWORKS FOR COLLISION AVOIDANCE AT INTERSECTIONS 7 (2011), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.710.412&rep=rep1&type=pdf; *see also* HARARI, *supra* note 46, at 23.

[48] FLORIDI, *supra* note 24, at 9.

[49] DENARDIS, *supra* note 3, at 46.

Transduction in information technologies is accomplished through sensors and actuators, either individually or in combination, in the following manner:

> Sensors detect and capture a signal from the real world (such as motion, sound, pressure, temperature, [or chemicals]), convert the signal to electrical form, and digitize and transmit this signal over a digital network . . . In contrast, an actuator is a device that 'acts' on the physical world, converting an electrical form into [information that instructs] tangible manipulation of the physical world.[50]

As a result, the veil between "*here* (*analogue, carbon-based, off-line*) and *there* (*digital, silicon-based, online*)" is rapidly dissolving.[51] Radically, transduction between the two worlds is bidirectional, with the digital world impacting the outer-analogue world and vis versa.[52]

With the means of cyber-physical communication identified, it is now time to introduce the Internet-of-Bodies.

B. THE INTERNET-OF-BODIES

The human body is now an information technology platform.[53] A new generation of internet-connected devices and sensors are being affixed to, embedded in, or ingested into the human body.[54] This new network of human bodies has been deemed the Internet-of-Bodies (IoB), and it is composed of "human bodies whose integrity and functionality rely at least in part on the Internet and related technologies, such as artificial intelligence."[55] IoB technologies can be categorized on a medical/non-medical spectrum as well as an invasive/non-

---

[50] *Id.*

[51] FLORIDI, *supra* note 24, at 16. (emphasis in original).

[52] DENARDIS, *supra* note 3, at 48.

[53] Xiao Liu & Jeff Merritt, *Shaping the Future of the Internet of Bodies: New challenges of technology governance*, WORLD ECONOMIC FORUM 7 (2020).

[54] *Id.*

[55] DENARDIS, *supra* note 3, at 80.

invasive spectrum.[56] An example of an invasive medical device includes a Food and Drug Administration-approved "internet-connected artificial pancreas [that acts] as an automated insulin delivery system for diabetes patients."[57] An example of a non-invasive, non-medical device is the now ubiquitous internet-connected smartwatch that acts as a personal fitness tracker.[58] As an out-of-the-box example, a suit has been created "to extract heat from the human body and repurpose it for cryptocurrency mining."[59]

More saliently, as this paper focuses on the IoB-human mind nexus, the human mind/AI unification relies on brain control interfaces (BCI). BCIs are bidirectional transduction "devices that enable . . . users to interact with computers by mean[s] of brain-activity only."[60] Facebook, Microsoft, and Elon Musk's Neuralink are all developing BCIs.[61] BrainGate, an interdisciplinary research team, develops BCI devices that use, "micro-electrodes implanted into the brain . . . that [detect] the neural signals associated with the intent to move a limb [that] can be 'decoded' by a computer in real-time and used to operate external devices."[62] The Defense Advanced Research Projects Agency's (DARPA) Next-Generation Nonsurgical Neurotechnology (N3) program is developing "bi-directional brain-machine interfaces . . . [to be used in] national security applications such as control of unmanned aerial vehicles and active cyber defense systems or teaming with computer systems to successfully multitask during complex military

---

[56] Liu & Merritt, *supra* note 53, at 7.

[57] *Id.* at 8.

[58] Alex Colon & Angela Moscaritolo, *The Best Smartwatches for 2021*, PCMAG (Nov. 12, 2021, 11:00 PM), https://www.pcmag.com/picks/the-best-smartwatches.

[59] Matwyshyn, *supra* note 2, at 102.

[60] Alexandre Gonfalonieri, *A Beginner's Guide to Brain-Computer Interface and Convolutional Neural Networks*, TOWARDS DATA SCIENCE (Nov. 25, 2018, 11:03 PM), https://towardsdatascience.com/a-beginners-guide-to-brain-computer-interface-and-convolutional-neural-networks-9f35bd4af948.

[61] Matwyshyn, *supra* note 2, at 98.

[62] BRAINGATE, https://www.braingate.org/about-braingate/ (last visited Nov. 12, 2021).

missions."[63] Notably, DARPA's BCI "would not require surgery and would be man-portable, thus making the technology accessible to a far wider population of potential users."[64]

Another goal of these technologies is to cognitively enhance otherwise healthy humans by merging human intelligence and AI to make knowledge downloadable and uploadable.[65] This coming reality not only compounds and accelerates existing privacy and security concerns associated with current internet-connected devices but also creates new, more serious concerns. The IoB will create a groundswell of new biometric and human behavioral data[66] third-parties can use that more accurately infer human behavior and psychology to predict and influence human behavior.[67] Novel corporate software liability issues will arise because "computer code will be able to physically damage . . . human bodies at scale,"[68] and human autonomy, decisional privacy, and democratic governance will be vulnerable to third-party actors who bidirectionally "feed into" human bodies and brains.[69] Safeguarding personal autonomy and decisional privacy should be the central legal principle governing the IoB because IoB-human mind transduction nexus is the most consequential transduction nexus in a modern democracy. Two things are needed to effectuate this legal principle: an understanding of how current, non-IoB artificially intelligent technologies—motivated by market forces—undermine autonomy and threaten democracy, and a pragmatic understanding of how the IoB's underlying technological global infrastructure operates.

---

[63] Gopal Sarma, *Next-Generation Nonsurgical Neurotechnology*, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (Nov. 12, 2021, 11:05 PM), https://www.darpa.mil/program/next-generation-nonsurgical-neurotechnology.

[64] *Id.*

[65] Matwyshyn, *supra* note 2, at 113.

[66] Liu & Merritt, *supra* note 53, at 7.

[67] U.N. High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, ¶ 16, U.N. Doc. A/HRC/48/31 (Sept. 13, 2021).

[68] Matwyshyn, *supra* note 2, at 80.

[69] *Id.* at 163.

V. PART IV: CURRENT NON-IOB ARTIFICIALLY INTELLIGENT TECHNOLOGIES ARE ERODING INDIVIDUAL AUTONOMY AND THREATENING DEMOCRACY.

The IoB is emerging in an era dominated by two global trends: psychological and political. The psychological trend is humanity's new quest to attain immortality, happiness, and super-human abilities through bio- and info-technologies.[70] The political trend is the recent global rise in authoritarianism and decline in democracy, which has manifested in the United States.[71]

A. THE PSYCHOLOGICAL TREND FUELING BIO- AND INFO-TECHNOLOGY.

Until the second half of the twentieth century, humankind's struggle was predominantly against famine, plague, and war.[72] Since that time, the global spread of the market economy, the astonishing speed and power of scientific and technology developments, and the democratization of the world have largely removed these concerns from much of the earth's population.[73] In his groundbreaking work, *Homo Deus: A Brief History of Tomorrow*, historian Yuval Hariri details how the void left by conquering famine, plague, and war will be replaced in the twenty-first century with a new struggle utilizing bio- and info-technologies to extend life, increase happiness, and acquire super-human abilities.[74] The trend was brought about through medical advances, such as "genetic engineering, regenerative medicine and nanotechnology," which will greatly extend the average lifespan.[75] In addition, biochemical manipulations used in mental health treatments,

---

[70] HARARI, *supra* note 5, at 21.

[71] *Global Democracy has a Very Bad Year: The Pandemic Caused an Unprecedented Rollback of Democratic Freedoms in 2020*, THE ECONOMIST, https://www.economist.com/graphic-detail/2021/02/02/global-democracy-has-a-very-bad-year (last visited Nov. 12, 2021).

[72] HARARI, *supra* note 5, at 1.

[73] *Id.* at 21.

[74] *Id.*

[75] *Id.* at 25.

such as anti-depressants and mood stabilizers, will increase and new treatments "that strengthen political stability, social order and economic growth" will develop and be encouraged.[76] And lastly, in achieving the two prior goals, the human body and mind will be "upgrad[ed]" with super-human abilities through "biological engineering, cyborg engineering and the engineering of non-organic beings."[77] These psychological trends are fueling the birth of the IoB-human mind unification and will be the economic engine of the new century.

B. THE POLITICAL TREND AWAY FROM DEMOCRACY AND TOWARD AUTOCRACY.

Simultaneously, however, democracy is in decline, and authoritarianism is on the rise. The Economist Intelligence Unit's Democracy Index empirically evaluates the global "state of democracy . . . based on five measures—electoral process and pluralism, the functioning of government, political participation, democratic political culture and civil liberties."[78] The 2020 report found only "8.4% of the world's population live in a full democracy while more than a third live under authoritarian rule."[79] The aggregate score was the lowest recorded since 2006.[80] Freedom House's *Freedom in the World 2020 Report* charted the fourteenth consecutive year of global democratic decline,[81] with 25 of 41 established democracies suffering a decline in the last year.[82] According to the report, the

---

[76] HARARI, *supra* note 5, at 41.
[77] *Id.* at 43.
[78] *Global Democracy has a Very Bad Year: The Pandemic Caused an Unprecedented Rollback of Democratic Freedoms in 2020*, THE ECONOMIST, https://www.economist.com/graphic-detail/2021/02/02/global-democracy-has-a-very-bad-year (last visited Nov. 12, 2021).
[79] *Id.*
[80] *Id.*
[81] Sarah Repucci et al, *Freedom in the World 2020: The Annual Survey of Political Rights & Civil Liberties*, FREEDOM HOUSE (Nov. 19, 2020, 9:54 AM), https://freedomhouse.org/sites/default/files/2021-08/FIW2020_book_JUMBO_PDF.pdf.
[82] *Id.* at 8.

United States dropped eight points in the last ten years, and it has fallen below its traditional democratic peers.[83]

C. TECHNOLOGY'S ROLE IN ERODING INDIVIDUAL AUTONOMY AND DEMOCRACY.

Current AI technologies, such as the various social media platforms, play a role in the decline of democracy and in undercutting personal autonomy. A Pew Research Center survey of tech experts distills the multi-varied causes for this. Forty-nine percent (49%) of respondents predicted that technology would continue to weaken democracy "due to the speed and scope of reality distortion, the decline of journalism and the impact of surveillance capitalism."[84]

Reality distortion is a product of algorithmic echo chambers and the viral spread of misinformation. Algorithms governing search queries, video suggestions, and social media connections use a consumer's past behavior to amplify what content that individual is exposed to, which is always at the expense of other viewpoints.[85] Once a user produces an algorithmic output, that output then becomes an input in the user's next use of the algorithm.[86] In this way, algorithms become active agents in influencing how users "perceive the world by filtering access to media; pushing political dialog towards extremes or filtering out contrary opinions."[87] According to internal Facebook research, "core product mechanics" such as "like" and "comment" functions, newsfeed content management algorithms, and content recommendation

---

[83] *Id.* at 6.

[84] Janna Anderson & Lee Rainie, *Many Tech Experts Say Digital Disruption Will Hurt* Democracy, PEW RESEARCH CENTER (Feb. 21, 2020), https://www.pewresearch.org/internet/2020/02/21/many-tech-experts-say-digital-disruption-will-hurt-democracy/.

[85] Swathi Meenakshi Sadagopan, *Feedback Loops and Echo Chambers: How Algorithms Amplify Viewpoints*, THE CONVERSATION (Feb. 4, 2019, 4:18 PM), https://theconversation.com/feedback-loops-and-echo-chambers-how-algorithms-amplify-viewpoints-107935.

[86] Grafanaki, *supra* note 18, at 825-26.

[87] Allison J.B. Chaney ET AL., *How Algorithmic Confounding in Recommendation Systems Increases Homogeneity and Decreases Utility*, ARXIV (2017), https://arxiv.org/pdf/1710.11214.pdf.

algorithms amplify misinformation and hate speech on the site.[88] The spread of misinformation on sites like Facebook has also led to a historical decline of trust in journalism.[89]

Surveillance capitalism and behavioral advertising are the hallmark elements of technology companies' business models. Tech companies provide free services as well as paid products in exchange for the ongoing collection of users' data. Companies use this data to create customer profiles, predict customer preferences and behaviors, and customize their services and third-party advertising to the customer.[90] The companies also directly monetize customer data and sell it to third-party data brokers. Altogether, this is known as surveillance capitalism.[91] Targeted behavioral advertising, whether incentivizing the purchase of consumer goods or garnering support or dislike of a political candidate, "can create psychological 'wants' that masquerade as cognitive choices."[92]

The loss of anonymity to surveillance capitalism and the unconscious manipulative power of algorithmic echo chambers, viral misinformation, and targeted behavioral advertising has weakened democratic institutions. Additionally, individuals have lost the power to make private, meaningful, authentic, and independent choices that are free from monitoring, interference, and categorization by others. The coming merger of bio- and info-technology at the IoB-human mind nexus raises the stakes dramatically because "[g]iven enough biometric data and enough computing power, external data-processing systems can hack . . . [an individual's] desires, decisions, and opinions."[93] To competently safeguard the human mind, it is necessary to build a comprehensive governing framework around a pragmatic understanding of the underlying technological architecture of the IoB.

---

[88] *The Facebook Papers and Their Fallout*, N.Y. TIMES (Oct. 25, 2021),

https://www.nytimes.com/2021/10/25/business/facebook-papers-takeaways.html?searchResultPosition=1.

[89] Manheim & Kaplan, *supra* note 17, at 150-51.

[90] Manheim & Kaplan, *supra* note 17, at 124.

[91] *Id.*

[92] Manheim & Kaplan, *supra* note 17, at 131.

[93] HARARI, *supra* note 46, at 51.

VI. PART V: A SNAPSHOT OF A GOVERNING FRAMEWORK THAT SAFEGUARDS PERSONAL AUTONOMY AND IS ROOTED IN TECHNOLOGY'S UNDERLYING GLOBAL ARCHITECTURE.

A pragmatic and principled IoB governing framework must secure its most vulnerable transduction node, the IoB-human mind nexus, and be rooted in the practical operation of technology's globally shared architectural underpinning. What follows is a comprehensive snapshot or survey of the proposed private market and governmental actions. Notably, the governing response advocated for in this paper synthesizes the work of Andrea Matwyshyn and Laura Denardis.

Andrea Matwyshyn, Penn State Professor of Law and Engineering Policy, argues that safeguarding personal autonomy and decisional privacy should be the central, permeating legal principle governing the IoB.[94] As Matwyshyn eloquently puts it:

> In a world where our bodies and minds are connected to a single interconnected technological network, we begin to blur the lines between the freedom of thought, i.e. the physiological and [externally unobservable] event of having a thought internally, and the act of broadcasting curated thoughts through the freedom of speech, i.e. the external autonomous manifestation that follows (or doesn't follow) a thought . . . For these reasons, our animating legal principle for IoB should reflect a focus on creating legal structures capable of safeguarding [inner thought] and the freedoms that emanate from it.[95]

To this end, laws responding to the IoB should recognize that authentic autonomous choices depend on "decisional privacy"[96] and "freedom from monitoring, scrutiny,

---

[94] Matwyshyn, *supra* note 2, at 164.

[95] *Id.*

[96] Manheim & Kaplan, *supra* note 17, at 145.

interference, and categorization by others."[97] Thusly, laws should ensure "independence of one's deliberation and choice from manipulation by"[98] private companies and state actors.

Laura DeNardis is a preeminent Internet governance scholar and American University professor in the School of Communication. In her recent work *The Internet in Everything; Freedom and Security in a World with No Off Switch*, DeNardis focuses on Internet and AI governance on five "[l]evers of control:" (1) design of behind-the-scenes technical architecture, (2) government legislation, regulation, and common law, (3) voluntary private sector enactments, (4) coordination between cross-border institutions, and (5) collective citizen action.[99] This section distills her perspective to introduce it into legal literature.

A. Private Sector Action as a Lever of Control

Necessary voluntary private-sector action centers on ensuring security and privacy-by-design at the time of product inception. This includes using highly secure cryptographic and blockchain technology to protect highly sensitive data,[100] ensuring software and security upgradability, regularly requiring manual password updates with multifactor authentication, restricting automatic Wi-Fi connections, and placing Internet-of-Things devices (of which IoB devices are a category) on separate firewalled networks.[101] Critically, data minimization should be a default practice. Under a data minimization regime, the "gathering, holding, using, and sharing of data" is limited to "the immediate purpose and context" of the specific task, "only shared beyond [that] purpose with clear and explicit consent."[102] Further actions include responsible "content moderation, [transparent] privacy terms of service, [data minimized] business models,"[103]

---

[97] Sofia Grafanaki, *Autonomy Challenges in the Age of Big Data*, 27 Fordham Intell. Prop. Media & Ent. L.J. 803, 809 (2017).
[98] Christman, *supra* note 12.
[99] DeNardis, *supra* note 3, at 18-9.
[100] *Id.* at 92.
[101] *Id.* at 120.
[102] *Id.* at 90.
[103] *Id. at* 19.

transparent data-breach disclosures,[104] end-to-end encryption with the prohibition of encryption back doors,[105] and the acquisition of consumer trust through "third-party rankings and certification[s]" demonstrating compliance with best privacy and security actions.[106] Public sector action should support and incentivize these actions, not undermine them.

B. CROSS-BORDER ACTION AS A LEVER OF CONTROL

Cross-border institution coordination involves setting device identification standards[107] as well as setting technical standards of interoperability. [108] Interoperability technical standards are "blueprints for . . . enabling networks and products built by different manufacturers to [exchange information] and incorporate . . . necessary [functions, such as] encryption, formatting, error checking, [and] addressing."[109]

Understanding the underlying structure of the Internet reveals how the privacy and security of each device and transduction node vitally rely on interoperability standards. The Internet is not a single cloud; rather, it is a collection of interconnected "private-sector-owned networks, routers, servers, buildings, switches, and fiber-optic cable . . . operated by different network operators and interconnected technical and economic (and sometimes political) agreements to interconnect and exchange information."[110]

Additionally, the Internet can be conceptualized as a network of layers with numerous types of protocol, with "[i]ssues of security transcend[ing] all layers."[111] One five-layer conceptualization includes:

> [*T*]*he physical* [*device*] *layer*, specifying mechanical, optical, or electrical interfaces between a device and a transmission medium

---

[104] *Id.* at 116.
[105] *Id.* at 125.
[106] *Id.* at 91.
[107] *Id.* at 54.
[108] *Id.* at 133.
[109] *Id.*
[110] *Id.* at 149-50.
[111] *Id.* at 139.

> (e.g., fiber-optic cable, coaxial cable, wireless); *the data-link layer*, such as Ethernet, providing logical specifications . . . for connecting to a network; *the network layer* . . . handling the assurance that packets successfully move from origination to destination point on a network; *the session and presentation layers* . . . for encoding and compressing information; and *the application layer*, which includes high-level protocols for email, file transfer, and web standards such as HTTP.[112]

Currently, a disparate proprietary product-by-product, company-by-company approach limiting interoperability is dominating the development of IoT and IoB. This approach has resulted in inconsistent degrees of protection within industries producing a less secure system overall. Denardis proposes interoperability within industry sectors but fragmentation by industry because "lack of cross-industry interoperability can serve as a check on security problems."[113] This is vital for the IoB, given the intimate nature of the biometric and behavioral data generated and the potential physical and mental consequences of device malfunction.

C. Design of Technical Architecture as a Lever of Control

Technical architecture takes into consideration the behind-the-scenes structure of the Internet, AI-operated autonomous and adaptive technologies, and points of vulnerability due to constrained energy, memory, and processing capabilities at nodes of control.[114] This level of control is exercised by identifying points of vulnerability within the interconnected operation of an IoB technology and ensuring as much security as physically possible at each point.

---

[112] *Id.* at 139 (emphasis added).
[113] *Id.* at 144.
[114] *Id.* at 52.

D. PUBLIC SECTOR ACTION AS A LEVER OF CONTROL

The United States (US) is legally ill-equipped for the IoB and human mind-AI unification. The US' legal approach to governing data protection and artificial intelligence can be considered sectorial at best and/or unaddressed at worst. The federal government does not have a comprehensive law, like the European Union, governing information privacy and security,[115] nor are there any federal, state, or local laws specific to artificial intelligence.[116] The US has "sector-specific federal laws and regulations," and a patchwork of state laws.[117] However, because courts regularly provide legal recourse for bodily injuries and contract disputes, the IoB will catalyze law formation around software liability, ownership,[118] and potentially malpractice under the theory that technology companies are professional information fiduciaries.[119]

E. FEDERAL STATUTES AND REGULATIONS

The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) will regulate IoB generated data that is categorized as "protected health information."[120] The Food and Drug Administration (FDA) has not promulgated any IoB specific regulations governing IoB medical devices though it has produced two guidance documents shifting the "agency toward greater scrutiny of IoB devices, particularly on security."[121] Matwyshyn urges the FDA to require premarket IoB technology disclosures enumerating "third-party code audit and testing, specifying any embedded code libraries, third-party hardware components, and comparable information," as well as requiring a "code safety warranty [that] extends to security," improving "its adverse [hacking or malfunctioning] event reporting structures and . . .

---

[115] Liu & Merritt, *supra* note 53, at 14.
[116] Manheim & Kaplan, *supra* note 17, at 160.
[117] Liu & Merritt, *supra* note 53, at 14.
[118] Matwyshyn, *supra* note 2, at 140.
[119] Grafanaki, *supra* note 18, at 842.
[120] Liu & Merritt, *supra* note 53, at 14.
[121] Matwyshyn, *supra* note 2, at 130-31.

public accessibility" thereof, and mandating the allowance of "independent forensic analysis of an IoB device following an adverse [hacking or malfunctioning] incident."[122]

The Federal Trade Commission Act, enforced by the Federal Trade Commission (FTC), forbids corporations from "engaging in deceptive or unfair acts or practices, including failing to comply with . . . [their] own privacy policy."[123] Because of the sensitive and bidirectional nature of IoB information, the IoB could catalyze the FTC to enforce the corporation's privacy policies aggressively. The FTC's Fair Information Practices Principles guide the federal government's sectoral approach to information privacy law.[124] Professor Matwyshyn recommends the FTC and FDA form a collaborative "'technologies practices' group, with a . . . cross-detailed team focused on IoB enforcement."[125]

Matwyshyn also emphasizes the unexplored role the Consumer Product Safety Commission (CPSC) and the Federal Communications Commission (FCC) could play in IoB governance.[126] The CPSC could create rules governing the safety of IoB hardware and software.[127] Lastly, the FCC's approach to the development of Internet infrastructure is implicated because IoB devices rely on Internet-connectivity for operation and security and could potentially cause grave harm due to poor connectivity.[128]

F. The United States' Patchwork of State Privacy Laws.

California, Illinois, and New York provide the most informative examples of proactive state privacy laws. Unfortunately, many states have left data privacy unaddressed. The Illinois Biometric Privacy Act (BIPA) is "the most comprehensive state biometric privacy law[]," notably providing individuals an actionable privacy violation cause

---

[122] *Id.* at 131-32.
[123] Liu & Merritt, *supra* note 53, at 14.
[124] *Id.*
[125] Matwyshyn, *supra* note 2, at 134.
[126] *Id.* at 135-38.
[127] *Id.* at 136.
[128] *Id.* at 137-38.

even if no actual harm results.[129] New York enacted the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) which compels any person or business owning or licensing personal data of a New York citizen to provide "reasonable safeguards to protect the security, confidentiality and integrity of the private information."[130] Both state's laws are directly relevant to IoB derived information and should help guide the development of federal and state data privacy and security legislation.

California's Online Privacy Protection Act of 2003 (CalOPPA) and the California Consumer Privacy Act (CCPA) compose the most comprehensive data privacy and security regime in the United States. The regime "requires operators of online services that collect 'personally identifiable information' (PII) to [publicly] post privacy policies that include: what data they are collecting, whom they are sharing it with, how to review or request changes to PII, and how users will be notified of policy changes."[131] The California laws also protect purchasing history data; browsing and search history data; and personality, behavioral, and political inferences drawn from PII.[132]

Additionally, California's regime created four new rights for citizen's individual control of data: (1) the right to delete one's data, (2) the right to "receive information and copies of [one's] data," (3) the right to opt-out of data collection, and (4) the right to "be free from [data-generated] discrimination."[133]

Just last year, California passed laws specific to IoT devices and chatbots. For example, IoT or smart device manufacturers "must implement reasonable security features preventing unauthorized access, information disclosure, or modification . . . chatbots must identify themselves and cannot pretend to be a real person . . . [and] . . . are prohibited from incentivizing the purchase or sale of goods and services and influencing an election vote."[134] California's law provides the

---

[129] Liu & Merritt, *supra* note 53, at 15.

[130] *Id.*

[131] Manheim & Kaplan, *supra* note 17, at 163-64.

[132] *Id.* at 164.

[133] *Id.*

[134] *Id.*

blueprint for future IoB legislation and directly addresses the role of artificial intelligence in undermining personal autonomy and democracy.

G. Tort, Contract, and Malpractice Law

Traditional tort, contract, and (potentially) malpractice law will help govern the IoB. IoB products will inevitably malfunction and cause physical bodily harm. Therefore, courts will have the potential to apply numerous theories of tort law. Accordingly, scholarship should explore how courts should approach duty and fact-specific inquiries into proximate causation, as these areas are uncharted and will likely not be consumer friendly.[135] Regarding contract law, the default approach taken with information technologies is consumer self-management under the paradigm of notice and consent end-user license agreements.[136] However, these contracts of adhesion are wholly inadequate and disproportional to the grave security and personal injury issues presented by the IoB. Provocatively, law professor Frank Pasquale[137] and others[138] have argued that "as algorithmic authorities get to know us better, at some point personalization becomes a relationship mutual enough to trigger the classic duties of professional [fiduciaries]."[139] This is an immensely alluring and creative approach to governing the IoB. The IoB-human mind nexus will provide algorithms and corporations with unprecedently intimate data. Imposing fiduciary duties upon technology companies will provide a market incentive for security- and privacy-by-design at the inception of IoB products.

VII. Conclusion

This paper has attempted to sound an alarm warning of the coming IoB-human mind nexus and its threats to personal autonomy and democratic governance. Furthermore, this paper

---

[135] Matwyshyn, *supra* note 2, at 139.
[136] Liu & Merritt, *supra* note 53, at 20.
[137] Grafanaki, *supra* note 18, at 842.
[138] Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 Md. L. Rev. 439 (2020).
[139] Grafanaki, *supra* note 18, 842.

proffered a scientific image of the informational nature of humans and artificially intelligent technologies to emphasize the practical reality of the IoB and to stress the ominous consequences resulting from the IoB-human mind nexus. Finally, in response to the concerns raised, this paper has provided a comprehensive Internet and AI governance snapshot focused on protecting human autonomy by being firmly grounded in the global technological architecture of the IoB and US law.