California Western Law Review

Volume 55 | Number 1 Article 5

12-20-2018

# The Internet of Bodies: Life and Death in the Age of AI

Eleonore Pauwels

Sarah W. Denton

FINAL Pauwels camera ready (Do Not Delete) 1/10/2019 11:10 AM

# THE INTERNET OF BODIES: LIFE AND DEATH IN THE AGE OF AI

ELEONORE PAUWELS* AND SARAH W. DENTON**

## TABLE OF CONTENTS



## I. INTRODUCTION

The fourth industrial revolution—characterized by technological advances in genomics and cyber-technologies including artificial intelligence ("AI"), automation, gene-editing, and neuroscience—seeks to merge our physical, digital, and biological lives. Yet, the Internet of Bodies exposes us to unprecedented privacy and cybersecurity vulnerabilities, introducing conflict across regulatory regimes. Now, societies must open a dialog to begin identifying the human values and

* Eleonore Pauwels is the Research Fellow on Emerging Cybertechnologies at the United Nations University's Center for Policy Research and the Director of the AI Lab within the Science and Technology Innovation Program at the Wilson Center. Her research focuses on the governance and democratization of converging technologies and how AI, genome-editing, and cyber-biosecurity raise opportunities and challenges across sectors.

** Sarah W. Denton is a research assistant in the Science and Technology Innovation Program at the Wilson Center and a Research Fellow at the Institute for Philosophy and Public Policy at George Mason University.

norms that will define responsible AI governance and data optimization.

> It's 6am and your AI personal assistant Niko greets you. As you walk into the bathroom, Niko connects to your smart mirror to analyze your saliva and biometric data to identify subtle changes in your health. Your life-cycle user platform is reflected around your face, – height 5'11", weight 157lbs, blood pressure 139/99 – quantifying your health in real-time via the Aegis implant in your arm. Streamed to the cloud, these biological data track your health, connect with physicians, and build powerful datasets for precision medicine.
>
> In an instant, the Aegis profile disappears, leaving your reflection seemingly bare. Then, Niko reminds you that your driverless car is arriving in 30 minutes. Your location is a core data point, which the Aegis constantly updates, sending data to the cloud every five minutes.
>
> En route to the office, you notice cameras equipped with facial and biometrics recognition software installed in each streetlight. They are part of the new City Brain, a comprehensive cognitive network that records and rates everyone's behaviors and interactions.[1]

Privacy is a concept that has existed—and evolved—as long as man and woman have roamed the earth. Indeed, questions concerning what *is* private and what *should* be private have been asked throughout time. The answers often updated across eras, cultures, and contexts. Though the above-recounted vision of 2075 may never be realized, today, personal privacy is now being questioned on terms unknown to previous generations. Increasingly, a world of devices connected to the internet will begin working with artificial intelligence to form personal algorithmic avatars of us all. We may soon be facing a privacy problem that we—literally—cannot keep to ourselves.

Artificial intelligence, commonly referenced in acronym form, is a term that would have sounded entirely self-contradictory before its birth

1. SARAH W. DENTON & ELEONORE PAUWELS, THERE'S NOWHERE TO HIDE: ARTIFICIAL INTELLIGENCE AND PRIVACY IN THE FOURTH INDUSTRIAL REVOLUTION 2 (2018), https://www.wilsoncenter.org/sites/default/files/ai_and_privacy.pdf.

in the 1950s.[2] Even today, many have trouble imagining how a machine could think or learn—abilities we inextricably associate with living beings. The term generally refers to "the use of digital technology to create systems that are capable of performing tasks commonly thought to require intelligence."[3] Machine learning, usually considered a subset of AI, describes "the development of digital systems that improve their performance on a given task over time through experience."[4] Deep neural networks are machine-learning architectures designed to mirror the way humans think and learn. At its core, AI optimizes data. Its machine-learning algorithms are trained to predict various aspects of our daily lives and, in the process, reveal hidden insight by making sense of massive amounts of information curated by humans.

The result? Functional capabilities that were previously unimaginable are now real, upgrading industries from defense and education to medicine and law enforcement. Companies, like Zipline, are using AI technology in autonomous drones to deliver crucial medical supplies to rural hospitals in Africa.[5] Police are harnessing AI's predictive power to both identify crime hotspots[6] and sort through faces in a crowd in real time.[7] AI empowers high-efficiency "smart

2. Rockwell Anyoha, *The History of Artificial Intelligence*, HARV. U. GRADUATE SCH. ARTS & SCI.: BLOG (Aug. 28, 2017), http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/.

3. Miles Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, at 9 (Feb. 2018), https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf.

4. *Id.*

5. *See, e.g.*, ZIPLINE, http://www.flyzipline.com/ (last visited Dec. 3, 2018); *Frequently Asked Questions*, ZIPLINE, http://www.flyzipline.com/faq/ (last visited Dec. 3, 2018).

6. PREDPOL, THE SCIENCE BEHIND PREDPOL, https://cdn2.hubspot.net/hubfs/3362003/White%20Paper%20Science%20&%20Testing%20of%20Predictive%20Policing.pdf (last visited Dec. 3, 2018).

7. *Smart System: Fire Eye Big Data Platform*, CLOUD WALK, http://www.cloudwalk.cn/product_detail_840.html (last visited Dec. 3, 2018) (use an in-browser translator).

cities."[8] It helps businesses minimize waste.[9] And it helps countries wage war.[10] Possibilities abound, both heartening and troubling. To stay on the sunny side for a moment, AI could become a powerful tool for development, akin to a new technological diplomacy; think of the goodwill engendered when a country or company makes available an image-recognition application that uses AI to help farmers identify diseases that affect their crops.[11] What we are currently witnessing is just the beginning of the AI revolution.

This article sheds light on the need for society to implement a set of standards for global regulation of AI, in an age where privacy concerns are evaporating as the Internet of Bodies grows. Part II shows the way in which society can collect the data needed for artificial intelligence and data optimization, at the expense of individual privacy. Part III highlights the effects AI and the Internet of Bodies will have on the diminishing boundaries between public and private life. Part IV explains the dangers and vulnerabilities of a fully implemented Internet of Bodies and AI structure. Finally, Part V discusses the differing approaches to AI governance in the United States, European Union, and China.

8. *See* Jacob Morgan, *A Simple Explanation of 'The Internet of Things,'* FORBES (May 13, 2014, 12:05 AM), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#1c32977f1d09; *see also* IEEE, SMART CITIES (2017), https://smartcities.ieee.org/images/files/pdf/IEEE_Smart_Cities_Flyer_Nov_2017.pdf.

9. *See generally* Julie Yamamoto, *4 Ways AI Helps Business Protect the Environment*, GREENBIZ (June 15, 2017, 2:00 AM), https://www.greenbiz.com/article/4-ways-ai-helps-business-protect-environment; Chad Pollitt, *How AI is Helping to Reduce Waste in Digital Advertising*, SOC. MEDIA TODAY (June 19, 2018), https://www.socialmediatoday.com/news/how-ai-is-helping-to-reduce-waste-in-digital-advertising/525980/.

10. *Artificial Intelligence in Modern Warfare: Impact and Future by Geography, Trends, Forecast*, REUTERS (July 25, 2017, 11:30 AM), https://www.reuters.com/brandfeatures/venture-capital/article?id=13524 (discussing the findings of a January 2017 report, published by Mordor Intelligence for Orbis Research, regarding the growth in the market for AI used for modern warfare).

11. Amanda Ramcharan & David Hughes, *Protecting Cassava from Disease? There's an App for That*, SCI. AM. (Jan. 31, 2018), https://www.scientificamerican.com/article/protecting-cassava-from-disease-there-rsquo-s-an-app-for-that/.

## II. THE NETWORKS OF OUR LIVES

But how, your non-artificially intelligent mind may be wondering, are we going to collect that massive amount of data to feed AI? A primary way is through the Internet of Things, or IoT, a term that future-of-work expert, Jacob Morgan, describes as "the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other)."[12] He continues: "This includes everything from cellphones [to] coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig."[13] In short, IoT refers to a constellation of billions of devices offering exponentially more data points on how things perform and how the world spins.[14] It's so large, and so seemingly innocuous, that you are probably unaware of its existence. But this pervasive network of sensors that captures data within our homes and cities is also in the process of morphing[15]—and this is where the privacy issue really gets personal.

The all-encompassing capture of our personal information—even the subtle quirks that make us who we are—will increasingly be used for various purposes without our direct knowledge or consent. On an individual level, our privacy is receding, and we are being exposed. AI's constant evolution parallels the technical advances in fields such as genomics, epidemiology, and neuroscience. As a result, not only is your coffee maker and your plane's engine sending information to the cloud, but so are wearable sensors like Fitbits, intelligent implants inside and outside our bodies, brain-computer interfaces, and even portable DNA sequencers. When optimized using AI, this trove of data provides superior information to fuel truly life-saving innovations. Consider research studies conducted by Apple and Google: the former's Heart Study app "uses data from Apple Watch to identify irregular heart rhythms, including those from potentially serious heart conditions such

12. Morgan, *supra* note 8.
13. *Id*.
14. *Id*.
15. *Id*.

as atrial fibrillation,"[16] while the Google-powered Project Baseline declares, "[w]e've mapped the world. Now let's map human health."[17] Never before have humans been equipped to monitor and sift through human behaviors and physiology on such a grand scale. We might call this set of networks the "Internet of *Living* Things (IoLT)," or the "Internet of Bodies."

There is great promise here, but also great peril, especially when considering ownership and control of our most intimate data. When computer codes analyze not only shopping patterns and dating preferences, but our genes, cells, and vital signs, your digital story takes its place within an array of fast-growing and increasingly interconnected databases of biometrics, faces, genomes, and behaviors. The digital representation of your characteristic data could help create the world's largest precision medicine dataset—or it could render everyone more vulnerable than ever before to a host of exploitations and intrusions. What might governments do with such information and capabilities? How might large corporations, using their vast computing and machine-learning platforms, try to commodify the streams of information about humans and ecosystems? Indeed, behavioral and biological features are beginning a new life on the internet, often with uncertain ownership and an uncertain future.

## III. A NEW CYBER-BIOPOWER

At the end of the electrifying 1970s in France, Michel Foucault coined the term "biopower" to describe how nation-states rely on an "explosion of numerous and diverse techniques for achieving the subjugation of bodies and the control of populations."[18] The ongoing digital and AI revolution magnifies his concerns.[19] While we are not

16. *Apple Heart Study*, STAN. MED., http://med.stanford.edu/appleheartstudy.html (last visited Dec. 3, 2018).

17. PROJECT BASELINE, https://www.projectbaseline.com/ (last visited Dec. 3, 2018).

18. Rachel Adams, *Michel Foucault: Biopolitics and Biopower*, CRITICAL LEGAL THINKING (May 10, 2017), http://criticallegalthinking.com/2017/05/10/michel-foucault-biopolitics-biopower/.

19. *See, e.g.*, John Cheney-Lippold, *A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control*, 28 THEORY, CULTURE & SOC'Y 164, 164-65 (2011), http://cmap.javeriana.edu.co/servlet/SBReadResourceServlet?rid =1N3N65Y7L-15LKRZW-57X; Thiago Mota, *The Agnostics of Life in the Age of Cyber-*

entering an Orwellian world or a dystopian episode of *Black Mirror* just yet, we cannot and should not ignore that the weakening boundary—and the weakening *distinction*—between "private" and "public" is a reality.

The repercussions of that weakening boundary showcase in China. Consider the Chinese students whose pictures and saliva samples were collected on campus to feed a database of faces and genomes.[20] Cloud Walk, a Chinese facial recognition software company, is developing AI technology that tracks individuals' movements and behavior to assess their chances of committing a crime.[21] Chinese police forces have debuted AI-augmented glasses that identify individuals in real time.[22] Notably, however, Chinese citizens are beginning to resist these breaches of personal privacy in the name of state-determined collective security.[23]

---

*biopower: Foucault, Negri and Hardt on Biopolitics and Intellectual Property Disputes*, ACADEMIA, http://www.academia.edu/14626946/The_Agonistics_of_Life_in_the_Age_of_Cyber-biopower_Foucault_Negri_and_Hardt_on_Biopolitcs_and_Intelectual_Property_Disputes (last visited Dec. 3, 2018).

20. Wenxin Fan et al., *China Snares Innocent and Guilty Alike to Build World's Biggest DNA Database*, WALL STREET J. (Dec. 26, 2017, 8:52 PM), https://www.wsj.com/articles/china-snares-innocent-and-guilty-alike-to-build-worlds-biggest-dna-database-1514310353.

21. *See* Yuan Yang et al., *China Seeks Glimpse of Citizens' Future with Crime-Predicting AI*, FIN. TIMES (July 23, 2017), https://www.ft.com/content/5ec7093c-6e06-11e7-b9c7-15af748b60d0; Simon Denyer, *China's Watchful Eye: Beijing Bets on Facial Recognition in a Big Drive for Total Surveillance*, WASH. POST (Jan. 7, 2018), https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance; *Smart System: Fire Eye Big Data Platform*, *supra* note 7. However, China is not the only place employing technology in this way: Chicago developed a "Strategic Subject List" using AI, which "analyzes people who have been arrested for their risk of becoming future perpetrators" by ranking them based on a variety of factors. Darrell M. West & John R. Allen, *How Artificial Intelligence is Transforming the World*, BROOKINGS (Apr. 24, 2018), https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/.

22. Josh Chin, *Chinese Police Add Facial-Recognition Glasses to Surveillance Arsenal*, WALL STREET J. (Feb. 7, 2018, 6:52 AM), https://www.wsj.com/articles/chinese-police-go-robocop-with-facial-recognition-glasses-1518004353.

23. Kenneth N. Farrall, *Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S.*, 2 INT'L J. COMM. 993, 1009, 1019 (2008), https://ijoc.org/index.php/ijoc/article/view/370/228 (discussing surveys showing

There are other examples beyond China in which governments and companies are tapping into the Internet of Bodies, sometimes without informed consent or democratic deliberation. The National Institution for Transforming India, also called NITI Aayog, is helping the Indian government aggregate private and public data on projects ranging from optimization of agriculture to healthcare.[24] The Indian government also mandated compliance with the creation of a country-wide biometrics database as part of Aadhaar's identification profile.[25] What India intends to do if and when it applies AI technology to such a database is uncertain. What *is* certain is that national and international governance structures are not well-equipped to handle the emerging concerns over privacy, ownership, and ethics.[26]

Could the Internet of Bodies and AI be used toward the "optimization" of the next generation's biology in line with prescribed ideals? The emergence of at-home genetic—and DNA—sequencing services, such as 23andMe,[27] has spurred complimentary services like InsideDNA, a cloud-based platform that features over 1,000 bioinformatics tools.[28] What if governments begin mandating

growing concern among the Chinese about privacy, including opposition real-name registration for blogs).

24. *See* NITI AAYOG, NATIONAL STRATEGY FOR ARTIFICIAL INTELLIGENCE: #AIFORALL 24-41 (2018), http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf; *Overview*, NITI AAYOG, http://niti.gov.in/content/overview (last updated Apr. 12, 2017, 1:44 AM).

25. Shashank Bengali, *India is Building a Biometric Database for 1.3 Billion People—and Enrollment is Mandatory*, L.A. TIMES (May 11, 2017, 3:00 AM), http://www.latimes.com/world/la-fg-india-database-2017-story.html. "Modeled after the American Social Security Number (SSN), the Aadhaar is a 12-digit unique identification number given to Indian citizens. The difference between the SSN and Aadhaar is the use of biometric data (fingerprints and iris scans) for verifying identity." Siddharthya Roy, *Aadhaar: India's Flawed Biometric Database*, DIPLOMAT (Mar. 6, 2018), https://thediplomat.com/2018/03/aadhaar-indias-flawed-biometric-database/.

26. *See*, *e.g.*, Amitabh Sinha, *Understanding the New DNA Tech Bill: All Your Questions Answered*, INDIAN EXPRESS (Aug. 1, 2017, 9:05 AM), https://indianexpress.com/article/explained/simply-put-understanding-the-new-dna-tech-bill-4776304/ (discussing privacy concerns and the potential of misuse of DNA samples collected in India).

27. 23ANDME, https://www.23andme.com/ (last visited Dec. 3, 2018).

28. INSIDEDNA, https://insidedna.io/ (last visited Dec. 3, 2018).

compliance with national genetic testing regimes? What will happen when AI converges with genome-*editing* technology?

And what of the afterlife in our AI world? Does this realm remain "private"? It turns out that power over our cyber-biological lives does not even vanish upon death.[29] Today, an industry flourishes around "deep fakes," forging speech and images to impersonate individuals—including deceased ones.[30] Think of chat bots that harness people's social media footprints to become online ghosts but apply that to humans. One AI startup, Luka, has launched a program that allows the public to engage with the co-founder's friend who was killed in a car accident.[31] A recent Oxford study calls for thorough ethical guidelines, arguing that "digital remains should be treated with the same care and respect as physical remains . . . ."[32]

Reserving ethical judgement on a "post-privacy" world, societies, as a whole, will have to determine to what extent the very concept of privacy can be modernized so as not to break, but to stretch and accommodate, a reality that looks very different than it has in the past.[33]

---

29. *See Estate Planning – Are Your Digital Assets Protected*?, CAL. W. SCH. L.: FAC. NEWS (July 25, 2018, 4:00 PM), https://www.cwsl.edu/news/newsroom/faculty-news/2018/07/25/estate-planning—are-your-digital-assets-protected.

30. *See* Sara A. O'Brien, *Deepfakes are Coming. Is Big Tech Ready?*, CNN: BUSINESS (Aug. 8, 2018, 11:16 AM), https://money.cnn.com/2018/08/08/technology/deepfakes-countermeasures-facebook-twitter-youtube/index.html. "Deep fakes" is "a phrase that has been most often used to describe a genre of artificial-intelligence-generated pornography that makes celebrities appear to engage in sexual scenes they had nothing to do with," however, scholars "describe the generation of deep fakes more broadly as digital manipulation of sound, images, or video to impersonate someone or make it appear that a person did something—and to do so in a manner that is increasingly realistic, to the point that the unaided observer cannot detect the fake." Marc J. Blitz, *Lies, Line Drawing, and (Deep) Fake News*, 71 OKLA. L. REV. 59, 61 (2018) (internal quotations omitted).

31. *Roman Mazurenko: A Digital Avatar*, APPLE: APP STORE, https://itunes.apple.com/us/app/luka/id958946383?mt=8 (last visited Dec. 3, 2018).

32. *Digital Remains Should be Treated Like Physical Ones*, U. OXFORD: NEWS (Apr. 18, 2018), http://www.ox.ac.uk/news/2018-04-18-digital-remains-should-be-treated-physical-ones; *see* Carl Öhman & Luciano Floridi, *An Ethical Framework for the Digital Afterlife Industry*, 2 NATURE HUM. BEHAV. 318 (Apr. 9, 2018); Carl Öhman & Luciano Floridi, *The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry*, 27 MINDS & MACHINES 639 (2017).

33. "Old people, says Lily, believe in privacy. The young aren't as naïve. They accept that their lives are for mass consumption. At best, they try to control what

## IV. THE PRIVACY-SECURITY QUAGMIRE

As long as individuals and societies have had privacy concerns, they have also had security concerns. While state-sponsored cyberattacks and cyber-espionage are hardly new, the proliferation of internet-connected devices,[34] the growth of the Internet of Bodies, and current and future AI technology will only exacerbate existing cybersecurity vulnerabilities.[35] Highly complex, these vulnerabilities are often misunderstood, and, therefore, too often neglected. What if skilled hackers were able to penetrate smart-city technologies, DNA databases, or perhaps neural-imaging databases? These would be the holy grail of population-level datasets, encompassing everything from our daily activities to our mental and physical health statuses.

Equally troubling, rising tech platforms are often our last line of defense to ensure the security of the massive, precious datasets that fuel our e-commerce, and soon, our smart cities and much more. That is, the same multinationals that reign over data and its liquidity are also charged with cybersecurity—creating potential conflicts of interest on a global scale. The revelation that Facebook made the private data of about 87 million users available to the Trump campaign[36] fueled new levels of public anxiety about tech giants' ability to exploit our personal information.[37] That tension weighs against the fact that the private tech sector is also enabling most of the enormously positive benefits that AI can, and likely will, usher in for individuals and societies, from helping

---

piece of themselves to upload." Amy Nicholson, *Film Review: 'Assassination Nation,'* VARIETY (Jan. 22, 2018, 4:18 PM), https://variety.com/2018/film/reviews/assassination-nation-review-1202672940/.

34. Jamie Condliffe, *How to Get One Trillion Devices Online,* M.I.T. TECH. REV. (Sept. 20, 2017), https://www.technologyreview.com/s/608878/how-to-get-one-trillion-devices-online/.

35. Joseph S. Nye, *Billions of Devices Will Soon be Vulnerable to Cyberattack. But We're not Ready*, WORLD ECON. F. (Mar. 13, 2018), https://www.weforum.org/agenda/2018/03/how-will-new-cybersecurity-norms-develop.

36. Cecilia Kang & Sheera Frenkel, *Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users,* N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html.

37. Alexei Oreskovic, *Sergey Brin: Silicon Valley has Outgrown the Time of Being 'Wide-Eyed and Idealistic' About Tech and Needs to Show 'Responsibility, Care and Humility'*, YAHOO!: FIN. (Apr. 29, 2018), https://finance.yahoo.com/news/sergei-brin-silicon-valley-outgrown-174719375.html.

to predict natural disasters to finding new warning signs for disease outbreaks. Thinking about how to ensure data liquidity and security will become increasingly more important as governments aim to reap such benefits.

## V. GOVERNING THE AI RACE

Regardless of whether the government in question is totalitarian or democratic, security risks, if not the privacy and civil liberties of citizens, should be cause for action. As you might imagine, AI and data governance around the world is a highly variable landscape, and in many instances, regulation is seriously lagging technological advances.

In collaboration with the European Commission, a few nations in Europe—led by France, the United Kingdom, and Estonia—are currently delineating their positions on AI's intersection with data privacy, liquidity, and security. In April, twenty-five European countries pledged to ally forces to shape a "European approach"[38] to AI, clearly in effort to compete with American and Asian tech platforms.[39] Simultaneously, the EU's new regulatory approach to data privacy and security, the General Data Protection Regulation ("GDPR"), is intended to "protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy."[40] Data collection and processing is allowed if, and only if, valid consent is obtained. Meanwhile, some argue that the GDPR could hinder economic competition and innovation.[41]

---

38. James Blackman, *25 Countries Join forces in Major European Collaboration*, ENTERPRISE IOT INSIGHTS (Apr. 10, 2018), https://enterpriseiotinsights.com/20180410/channels/news/countries-join-forces-in-european-ai-collaboration-tag40; *see Commission Outlines European approach to Artificial Intelligence*, European Commission (Apr. 25, 2018), https://ec.europa.eu/growth/content/commission-outlines-european-approach-artificial-intelligence_en.

39. *See id.*; *see also* European Commission Press Release IP/18/3362, Artificial Intelligence: Commission Outlines a European Approach to Boost Investment and Set Ethical Guidelines (Apr. 25, 2018), http://europa.eu/rapid/press-release_IP-18-3362_en.htm.

40. *The EU General Data Protection Regulation (GDPR) is the Most Important Change in Data Privacy Regulation in 20 Years*, EU GDPR, https://eugdpr.org/ (last visited Dec. 3, 2018).

41. For example, according to the U.S. Federal Trade Commissioner, Noah Phillips, "Laws and regulations intended to promote privacy may build protective

While the EU has taken a broader, preventive approach to the misuse or unauthorized use of personal data, the U.S. has relied on responsive enforcement and industry self-regulation in the absence of any statue that holistically covers the subject.[42] Existing U.S. privacy law must be updated to reflect new realities facilitated by AI. The U.S. and China both remain largely silent in this area, seeking to protect their competitive advantage in technological innovation. Ultimately, new developments in data sharing and optimization will challenge both approaches and will require new tools to address the resulting privacy issues.

In China, which is increasingly challenging the U.S. position at the front of the AI pack, the state is implementing AI technologies for surveillance and customer service with particular rapidity. Though Beijing recently passed its cybersecurity law, which calls for storing data inside the country to protect internet-connected devices from security threats,[43] the law creates headaches for foreign-tech companies and its privacy protections fail to keep pace with the speed of innovation.[44]

## VI. CONCLUSION

In a stirring new op-ed, surprisingly on AI, Henry Kissinger writes that the contemporary world order "is now in upheaval amid a new, even more sweeping technological revolution whose consequences we

moats around large companies . . . making it more difficult for smaller companies to grow, for new companies to enter the market, and for innovation to occur[.]" Gary Arlen, *Privacy Policy Could Impeded Competition, Innovation, New FTC Commissioner Warns*, MULTICHANNEL (July 31, 2018), https://www.multichannel.com/blog/privacy-policy-could-impede-competition-innovation-new-ftc-commissioner-warns. Phillips went on to state that the GDPR's "early signs point to precisely the effects on competition that I fear." *Id*.

42. *America Should Borrow from Europe's Data-Privacy Law*, ECONOMIST (Apr. 5, 2018), https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law.

43. Jack Wagner, *China's Cybersecurity Law: What you need to know*, DIPLOMAT (June 1, 2017), https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/.

44. He Huifeng, *Cybersecurity Law Causing 'Mass Concerns' Among Foreign Firms in China*, SOUTH CHINA MORNING POST (Mar. 1, 2018, 10:38 PM), https://www.scmp.com/news/china/economy/article/2135338/cybersecurity-law-causing-mass-concerns-among-foreign-firms-china.

have failed to fully reckon with, and whose culmination may be a world relying on machines powered by data and algorithms and ungoverned by ethical or philosophical norms."[45] Competing interests and abundant complexities notwithstanding—or, rather, *because* of them—now is the time to collectively define a responsible way to govern AI and data-optimization within our democracies.[46]

Future conflicts over who owns, steals, or benefits from genetic secrets must be balanced by open-source efforts to ensure that data and this new generation of technological tools primarily serve the public good. An international network of technology leaders, ethicists, policymakers, members of civil society, and writers and artists, need to come together and articulate a set of globally applicable policies and norms that protect basic human and civil rights in the algorithmic age. They also need to be transparent and courageous, explaining to the public how AI and the Internet of Bodies is transforming our privacy and ourselves. Only then will we be able to determine how to design AI and related technologies in a socially responsible and sustainable manner.

45. Henry A. Kissinger, *How the Enlightenment Ends*, ATLANTIC (June 2018), https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/.

46. *See id.*