Artificial Intelligence: Risks to Privacy and Democracy

Karl Manheim[*] and Lyric Kaplan[**]

21 Yale J.L. & Tech. 106 (2019)

A "Democracy Index" is published annually by the Economist. For 2017, it reported that half of the world's countries scored lower than the previous year. This included the United States, which was demoted from "full democracy" to "flawed democracy." The principal factor was "erosion of confidence in government and public institutions." Interference by Russia and voter manipulation by Cambridge Analytica in the 2016 presidential election played a large part in that public disaffection.

Threats of these kinds will continue, fueled by growing deployment of artificial intelligence (AI) tools to manipulate the preconditions and levers of democracy. Equally destructive is AI's threat to decisional and informational privacy. AI is the engine behind Big Data Analytics and the Internet of Things. While conferring some consumer benefit, their principal function at present is to capture personal information, create detailed behavioral profiles and sell us goods and agendas. Privacy, anonymity and autonomy are the main casualties of AI's ability to manipulate choices in economic and political decisions.

The way forward requires greater attention to these risks at the national level, and attendant regulation. In its absence, technology giants, all of whom are heavily investing in and profiting from AI, will dominate not only the public discourse, but also the future of our core values and democratic institutions.

---

[*] Professor of Law, Loyola Law School, Los Angeles. This article was inspired by a lecture given in April 2018 at Kansai University, Osaka, Japan.

[**] Associate in Privacy & Data Security Group, Frankfurt Kurnit Klein & Selz, Los Angeles. The authors are grateful to Cornelia Dean, Tanya Forsheit, Justin Hughes, Justin Levitt, Yxta Murray, Elizabeth Pollman and Neil Sahota for their incredibly helpful comments on earlier drafts.

INTRODUCTION

Artificial intelligence (AI) is the most disruptive technology of the modern era. Its impact is likely to dwarf even the development of the internet as it enters every corner of our lives. Many AI applications are already familiar, such as voice recognition, natural language processing and self-driving cars. Other implementations are less well known but increasingly deployed, such as content analysis, medical robots, and autonomous warriors. What these have in common is their ability to extract intelligence from unstructured data. Millions of terabytes of data about the real world and its inhabitants are generated each day. Much of that is noise with little apparent meaning. The goal of AI is to filter the noise, find meaning, and act upon it, ultimately with greater precision and better outcomes than humans can achieve on their own. The emerging intelligence of machines is a powerful tool to solve problems and to create new ones.

Advances in AI herald not just a new age in computing, but also present new dangers to social values and constitutional rights. The threat to privacy from social media algorithms and the Internet of Things is well known. What is less appreciated is the even greater threat that AI poses to democracy itself.[1] Recent events illustrate how AI can be "weaponized" to corrupt elections and poison people's faith in democratic institutions. Yet, as with many disruptive technologies, the law is slow to catch up. Indeed, the first ever Congressional hearing focusing on AI was held in late 2016,[2] more than a half-century after the military and scientific communities began serious research.[3]

The digital age has upended many social norms and structures that evolved over centuries. Principal among these are core values such as personal privacy, autonomy, and democracy. These are the foundations of liberal democracy, the power of which during the late 20th

---

[1] *See* Nicholas Wright, *How Artificial Intelligence Will Reshape the Global Order*, FOREIGN AFF. (July 10, 2018), https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order.
[2] *See The Dawn of Artificial Intelligence: Hearing Before the Senate Committee on Commerce, Science & Transportation*, 115th Cong. 2 (2016), https://www.govinfo.gov/content/pkg/CHRG-114shrg24175/pdf/CHRG-114shrg24175.pdf ("This is the first congressional hearing on artificial intelligence.").
[3] AI began as a discrete field of research in 1956. *What Is Artificial Intelligence*, SOC'Y FOR STUDY OF ARTIFICIAL INTELLIGENCE & SIMULATION BEHAV., http://www.aisb.org.uk/public-engagement/what-is-ai (last visited Jan. 4, 2019).

century was unmatched in human history. Technological achievements toward the end of the century promised a bright future in human well-being. But then, danger signs began to appear. The internet gave rise to social media, whose devaluation of privacy has been profound and seemingly irreversible. The Internet of Things (IoT) has beneficially automated many functions while resulting in ubiquitous monitoring and control over our daily lives. One product of the internet and IoT has been the rise of "Big Data" and data analytics. These tools enable sophisticated and covert behavior modification of consumers, viewers, and voters. The resulting loss of autonomy in personal decision-making has been no less serious than the loss of privacy.

Perhaps the biggest social cost of the new technological era of AI is the erosion of trust in and control over our democratic institutions.[4] "Psychographic profiling" of Facebook users by Cambridge Analytica during the 2016 elections in Britain and the United States are cases in point. But those instances of voter manipulation are hardly the only threats that AI poses to democracy. As more and more public functions are privatized, the scope of constitutional rights diminishes. Further relegating these functions to artificial intelligence allows for hidden decision-making, immune from public scrutiny and control. For instance, predictive policing and AI sentencing in criminal cases can reinforce discriminatory societal practices, but in a way that pretends to be objective. Similar algorithmic biases appear in other areas including credit, employment, and insurance determinations. "Machines are already being given the power to make life-altering, everyday decisions about people."[5] And they do so without transparency or accountability.

Sophisticated manipulation technologies have progressed to the point where individuals perceive that decisions they make are their own, but are instead often "guided" by algorithm. A robust example

---

[4] *See, e.g.*, Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 195 (2017) (the AI-enabled "ecosystems constructed by Google and Facebook have contributed importantly to the contemporary climate of political polarization and distrust"); *infra* Section IV.A.4.

[5] Jonathan Shaw, *Artificial Intelligence and Ethics*, HARV.MAG. (Jan.-Feb. 2019), https://www.harvardmagazine.com/2019/01/artificial-intelligence-limitations.

is "big nudging," a form of "persuasive computing" "that allows one to govern the masses efficiently, without having to involve citizens in democratic processes."[6] Discouraged political participation[7] is one of the aims of those who abuse AI to manipulate and control us.[8]

Collectively and individually, the threats to privacy and democracy degrade human values. Unfortunately, monitoring of these existential developments, at least in the United States, has been mostly left to industry self-regulation. At the national level, little has been done to preserve our democratic institutions and values. There is little oversight of AI development, leaving technology giants free to roam through our data and undermine our rights at will.[9] We seem to find ourselves in a situation where Mark Zuckerberg and Sundar Pichai, CEOs of Facebook and Google, have more control over Americans' lives and futures than do the representatives we elect. The power of these technology giants to act as "Emergent Transnational Sovereigns"[10] stems in part from the ability of AI software ("West Coast Code") to subvert or displace regulatory law ("East Coast Code").[11]

---

[6] Dirk Helbing et al., *Will Democracy Survive Big Data and Artificial Intelligence?*, SCI. AM. (Feb. 25, 2017), https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence.

[7] *See* H. Akin Ünver, *Artificial Intelligence, Authoritarianism and the Future of Political Systems,* in CYBER GOVERNANCE AND DIGITAL DEMOCRACY 2018/9), http://edam.org.tr/wp-content/uploads/2018/07/AKIN-Artificial-Intelligence_Bosch-3.pdf at 4 (explaining that "non-transparent and non-accountable technology and information systems may lead to discouraged political participation and representation" by "reinforc[ing] centralized structures of control, rather than participation").

[8] Elaine Kamarck, *Malevolent Soft Power, AI, and the Threat to Democracy,* BROOKINGS, Nov. 28, 2018, https://www.brookings.edu/research/malevolent-soft-power-ai-and-the-threat-to-democracy (describing the use of technological tools to suppress the vote and "undo democracy in America and throughout the Western world.").

[9] *See generally* Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 HARV. J. L. & TECH 353 (2016) ("[T]he rise of AI has so far occurred in a regulatory vacuum.").

[10] Cohen, *supra* note 4, at 199. *See also* Ünver, supra note 7 (the "structures of automation . . . form a new source of power that is partially independent of states as well as international political institutions"); *infra* notes 77-78 (describing the economic power of technology companies rivaling that of countries).

[11] *See infra* note 379.

Some have described the emerging AI landscape as "digital authoritarianism"[12] or "algocracy"—rule by algorithm.[13]

This article explores present and predicted dangers that AI poses to core democratic principles of privacy, autonomy, equality, the political process, and the rule of law. Some of these dangers predate the advent of AI, such as covert manipulation of consumer and voter preferences, but are made all the more effective with the vast processing power that AI provides. More concerning, however, are AI's *sui generis* risks. These include, for instance, AI's ability to generate comprehensive behavioral profiles from diverse datasets and to reidentify anonymized data. These expose our most intimate personal details to advertisers, governments, and strangers. The biggest dangers here are from social media, which rely on AI to fuel their growth and revenue models. Other novel features that have generated controversy include "algorithmic bias" and "unexplained AI." The former describes AI's tendency to amplify social biases, but covertly and with the pretense of objectivity. The latter describes AI's lack of transparency. AI results are often based on reasoning and processing that are unknown and unknowable to humans. The opacity of AI "black box" decision-making[14] is the antithesis of democratic self-governance and due process in that they preclude AI outputs from being tested against constitutional norms.

We do not underestimate the productive benefits of AI, and its inevitable trajectory, but feel it necessary to highlight its risks as well. This is not a vision of a dystopian future, as found in many dire warnings about artificial intelligence.[15] Humans may not be at risk

---

[12] Wright, *supra* note 1.
[13] John Danaher, *Rule by Algorithm? Big Data and the Threat of Algocracy*, PHILOSOPHICAL DISQUISITIONS (Jan. 26, 2014), http://philosophicaldisquisitions.blogspot.com/2014/01/rule-by-algorithm-big-data-and-threat.html.
[14] *See* Will Knight, *The Dark Secret at the Heart of AI*, MIT TECH. REV. (Apr. 11, 2017), https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai (describing the "black box" effect of unexplainable algorithmic functions).
[15] *See, e.g.*, NICK BOSTROM, SUPERINTELLIGENCE: PATHS, DANGERS, STRATEGIES (2014), 115 ("[A] plausible default outcome of the creation of machine superintelligence is existential catastrophe.").

as a species, but we are surely at risk in terms of our democratic institutions and values.

Part II gives a brief introduction to key aspects of artificial intelligence, such that a lay reader can appreciate how AI is deployed in the several domains we discuss. At its most basic level, AI emulates human information sensing, processing, and response—what we may incompletely call "intelligence"—but at vastly higher speeds and scale—yielding outputs unachievable by humans.[16]

Part III focuses on privacy rights and the forces arrayed against them. It includes a discussion of the data gathering and processing features of AI, including IoT and Big Data Analytics. AI requires data to function properly; that means vast amounts of personal data. In the process, AI will likely erode our rights in both decisional and informational privacy.

Part IV discusses AI's threats to democratic controls and institutions. This includes not just the electoral process, but also other ingredients of democracy such as equality and the rule of law. The ability of AI to covertly manipulate public opinion is already having a destabilizing effect in the United States and around the world.

Part V examines the current regulatory landscape in the United States and Europe, and civil society's efforts to call attention to the risks of AI. We conclude this section by proposing a series of responses that Congress might take to mediate those risks. Regulating AI while promoting its beneficial development requires careful balancing. But that must be done by public bodies and not simply AI developers and social media and technology companies, as is mostly the case now.[17] It also requires AI-specific regulation and not just extension of existing law. The European Parliament has recently proposed one regulatory model and set of laws. We draw on that as well as ethical and democracy-reinforcing principles developed by the AI community itself. We are all stakeholders in this matter and

---

[16] For a general description of AI capabilities, see Scherer, *supra* note 9.

[17] Amazon and Alphabet each spent roughly three times as much on AI R&D in 2017 as total U.S. federal spending. *See* SHOHAM ET AL., *ARTIFICIAL INTELLIGENCE INDEX 2018 ANNUAL REPORT* at 58 (2018).

need to correct the asymmetry of power that currently exists in the regulation and deployment of AI.

Risks associated with artificial intelligence are not the gravest problem facing us today. There are more existential threats such as climate change.[18] But an ecosystem of reality denial that includes algorithmic targeting of susceptible groups and policy makers has even infected the debate about climate change.[19] AI is being used to sow seeds of distrust of government and democratic institutions, leading to paralysis of collective action.[20] The consequences can be disastrous. As Stephen Hawking, Elon Musk and Bill Gates have warned, artificial intelligence may be humanity's greatest invention but also imposes great risk.[21] This Article explores some of those risks. In that respect, it joins an emerging discourse warning of the disruptive power of AI and its destabilization of social structures.[22]

I. A BRIEF INTRODUCTION TO AI

Artificial intelligence is a form of "intelligent computing"[23] in that it relies on computer programs that can sense, reason, learn, act, and adapt much like humans do.[24] It is "intelligent" because it emulates

---

[18] *Cf.* Nathaniel Rich, *Losing Earth: The Decade We Almost Stopped Climate Change*, N.Y. TIMES (Aug. 1, 2018) ("Long-term disaster is now the best-case scenario.").

[19] *See, e.g.*, 163 Cong. Rec. S. 2970, May 16, 2017 (remarks of Sen. Whitehouse); Sander van der Linden, *Inoculating the Public Against Misinformation About Climate Change*, 1 GLOBAL CHALLENGES (2017).

[20] *See* Cohen, *supra* note 4. Distrust in institutions exacerbates the collective action problem in providing public goods such as environmental protection.

[21] *See* Kelsey Piper, *The Case for Taking AI Seriously As A Threat to Humanity*, VOX (Dec. 23, 2018, 12:38 AM), https://www.vox.com/future-perfect/2018/12/21/18126576/ai-artificial-intelligence-machine-learning-safety-alignment.

[22] *See, e.g.,* Hin-Yan Liu, *The Power Structure of Artificial Intelligence*, 10 L. INNOVATION & TECH. 197 (2018); Henry Kissinger, *How the Enlightenment End*s, ATLANTIC (June 2018), https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/ (arguing that "human society is unprepared for the rise of artificial intelligence").

[23] Computer scientists may call this "computational intelligence," of which AI is a subset.

[24] FUTURE of Artificial Intelligence Act, H.R. 4625, 115th Cong. § 3 (2017) contains a more detailed "official" definition that mostly tracks that provided

human cognition.[25] It is "artificial," because it involves computational rather than biological information processing. AI's emerging power derives from exponential growth in computer processing and storage, and vast repositories of data that can be probed to extract meaning. The computational abilities of machines and advances in robotics[26] are now so impressive that many science fiction predictions of the past seem to pale in comparison. With quantum computing on the near horizon,[27] the competencies of AI will improve faster than we can imagine or prepare for.

Many different systems fall under the broad AI umbrella. These include "expert systems," which are detailed algorithms (stepwise computer programs) containing a series of human-programmed rules and knowledge for problem solving. "Machine learning" (ML) is a more advanced form of AI that depends less on human programming and more on an algorithm's ability to use statistical methods and learn from data as it progresses. ML can either be "supervised" (human-trained) or "unsupervised," meaning that it is self-trained without human input.[28] An early application of the technology was developed in 1997 by two Stanford University students, Larry Page and Sergey Brin. They built a catalog of web rankings based on the frequency of incoming links. The search engine they built – Google – has evolved into one of the largest AI companies in the world.[29]

A strong form of ML is "Deep Learning" (DL), which uses learning algorithms called artificial neural networks that are loosely inspired

---

here. Among many works that describe AI in great detail, we recommend LUKE DORMEHL, THINKING MACHINES (Penguin, 2017) for an excellent overview that is accessible to lay readers.

[25] *See, e.g.*, *Algorithms Based On Brains Make For Better Networks*, NEUROSCIENCE NEWS (July 17, 2015), https://neurosciencenews.com/neuroscience-network-algorithms-2263.

[26] As we use the term, a robot is essentially AI with moving parts.

[27] *See* Vivek Wadhwa, *Quantum Computers May Be More of an Imminent Threat than AI*, WASH. POST (Feb. 5, 2018), https://www.washingtonpost.com/news/innovations/wp/2018/02/05/quantum-computers-may-be-more-of-an-imminent-threat-than-ai.

[28] *See generally* Nikki Castle, *Supervised vs. Unsupervised Machine Learning*, DATASCIENCE.COM (July 13, 2017), https://www.datascience.com/blog/supervised-and-unsupervised-machine-learning-algorithms.

[29] *See* DORMEHL, *supra* note 24. Google's AI operations have been restructured into its parent company, Alphabet, Inc.

by the structure of the human brain. Artificial neurons are connected to one another in layers that rewire and edit themselves on the fly through "backpropagation" feedback loops.[30] These emulate neural pathways in the brain, which strengthen themselves each time they are used.[31] This dynamic approach allows DL to find patterns in unstructured data, from which it models knowledge representation in a manner that resembles reasoning. With DL, developers input only basic rules (e.g., mathematical operations) and goals; the AI will figure out the steps necessary to implement them.[32] This ability to adapt is what makes AI so powerful.

The timeline for AI's capacity to surpass human intelligence is fiercely debated. What is known as the Turing Test is an experiment where a human interrogator is unable to distinguish between human and computer-generated natural-language responses in a blind conversation.[33] Futurist Ray Kurzweil has predicted successful passing of the Turing Test in 2029.[34] Until then, we remain in an era of Artificial Narrow Intelligence (ANI), or weak AI, where special-purpose computer programs outperform humans in specific tasks such as games of skill and text analysis. ANI includes cognitive computing where machines assist humans in the completion of tasks such

---

[30] *See* Alexx Kay, *Artificial Neural Networks,* COMP. WORLD (Feb. 12, 2001), https://www.computerworld.com/article/2591759/app-development/artificial-neural-networks.html. DL emulates neural networks in the human brain, which also make many, often random, connections for each action to optimize output.
[31] DORMEHL, *supra* note 24, at 35.
[32] *See* Alex Castrounis, *Artificial Intelligence, Deep Learning, and Neural Networks Explained*, INNOARCHITECH, https://www.innoarchitech.com/artificial-intelligence-deep-learning-neural-networks-explained ("[DL] algorithms themselves 'learn' the optimal parameters to create the best performing model … In other words, these algorithms *learn how to learn*.").
[33] *The Turing Test*, STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Apr. 9, 2003), https://plato.stanford.edu/entries/turing-test.
[34] The difficulty in predicting passage of the Turing Test is compounded by disagreements over means for measuring machine intelligence. In 2014, a chatbot fooled several human judges into thinking it was human, but this did not convince many scientists. Nadia Khomami, *2029: The Year When Robots Will Have the Power to Outsmart Their Makers*, GUARDIAN (Feb. 22, 2014), https://www.theguardian.com/technology/2014/feb/22/computers-cleverer-than-humans-15-years.

as helping radiologists read X-rays, stockbrokers make trades, and lawyers write contracts.[35]

The next generation of AI will be Artificial General Intelligence (AGI). Its capabilities will extend beyond solving a specific and predefined set of problems to applying intelligence to any problem.[36] Once computers can autonomously outperform even the smartest humans, we will have reached Artificial Super Intelligence (ASI).[37] Some have described this as the "singularity," when the competences of silicon computing will exceed those of biological computing.[38] At that point, visions of a dystopian future could emerge.[39] Fortunately, we have time to plan. Unfortunately, we are lacking an appropriate sense of urgency.

II. THREATS TO PRIVACY

The right to make personal decisions for oneself, the right to keep one's personal information confidential, and the right to be left alone are all ingredients of the fundamental right of privacy. These rights are commonly recognized and protected in many post-World War II charters on human rights and are considered core precepts of democracy.[40] The U.S. Constitution indirectly recognizes the rights of decisional and informational privacy, although such recognition stems

---

[35] *See* J.C.R. Licklider, *Man-Computer Symbiosis*, 1 IRE TRANSACTIONS HUMAN FACTORS ELEC. 4, 4 (1960).
[36] Joel Traugott, *The 3 Types of AI: A Primer*, ZYLOTECH (Oct. 24, 2017), https://www.zylotech.com/blog/the-3-types-of-ai-a-primer.
[37] BOSTROM, *supra* note 15.
[38] *See* RAY KURZWEIL, THE SINGULARITY IS NEAR 136 (2005). John Von Neumann used this term to describe the point of technological progress "beyond which human affairs, as we know them, could not continue." Stanislaw Ulam, *Tribute to John Von Neumann*, 64 BULLETIN AM. MATHEMATICAL SOC'Y 1, 5 (1958).
[39] *See* BOSTROM, *supra* note 15. Kurzweil predicts this to occur circa 2045. *See* KURZWEIL, *supra* note 38.
[40] *See, e.g.,* Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948), Art. 12; Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, as amended by Protocols Nos. 11 and 14, 4 November 1950, Art. 8; Organization of American States (OAS), *American Convention on Human Rights*, "Pact of San Jose", Costa Rica, 22 November 1969, Art. 11.

largely from judicial inference rather than textual command.[41] As we will shortly see, the weak protections given privacy rights in U.S. constitutional and statutory law invite creative and frequent invasion of those rights. This Part discusses those problems and the added threats that AI poses.

A. Forms of Privacy

The seminal work on information privacy is Samuel Warren and Louis Brandeis' 1890 article "The Right to Privacy,"[42] which surveyed and furthered the development of the common law "right of the individual to be let alone." As privacy rights developed in the courts over the years, William Prosser crystalized four distinct harms arising from privacy violations: 1) intrusion upon seclusion or solitude, or into private affairs; 2) public disclosure of embarrassing private facts; 3) false light publicity; and 4) appropriation of name or likeness.[43] Today, most states recognize the four-distinct harms as privacy-related torts and provide civil and criminal remedies for the resulting causes of action. The privacy torts aim to protect people whose sensibilities and feelings are wounded by having others uncover truthful, yet intimate or embarrassing facts due to highly offensive conduct.[44]

---

[41] The Fourth Amendment contains the only explicit reference to information privacy: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated. . . ." The "right of privacy" in common parlance usually refers to decisional privacy. Judicial recognition appears in cases such as Griswold v. Conn., 381 U.S. 479 (1965) (marital privacy) and Roe v. Wade, 410 U.S. 113 (1973) (right to abortion). The right to information privacy was assumed in Whalen v. Roe, 429 U.S. 589 (1977) (upholding mandated reporting of patient prescriptions), but questioned in NASA v. Nelson, 562 U.S. 134 (2011) (upholding unconsented background checks, including medical information, of federal employees).

[42] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). They were apparently influenced by George Eastman's development of a portable camera, and its' marketing to ordinary consumers by the Kodak Company, fearing its ability to capture images of private matters.

[43] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

[44] Anita L. Allen-Castellitto, *Understanding Privacy: The Basics,* 865 PLI/PAT 23 (2006).

Beyond the common law origins of privacy and personality lay other conceptions of privacy. These include informational privacy, decisional privacy, behavioral privacy, and physical privacy.[45] Informational privacy is the right to control the flow of our personal information. It applies both to information we keep private and information we share with others in confidence.[46] Decisional privacy is the right to make choices and decisions without intrusion or inspection.[47] Behavioral privacy includes being able to do and act as one wants, free from unwanted observation or intrusion.[48] Physical privacy encompasses the rights to solitude, seclusion, and protection from unlawful searches and seizures.[49] These conceptions of privacy have become a central feature of Western democracy as reflected by their incorporation into foundational documents and a large body of statutory, common, and evidentiary laws.

Informational privacy promotes a number of democratic values: the capacity to form ideas, to experiment, to think or to make mistakes without observation or interference by others. It also protects other freedoms including political participation, freedom of conscience, economic freedom, and freedom from discrimination.

Loss of information privacy can erode those same freedoms. When others have access to our private information, they may be able to influence or control our actions. That is why so many actors seek to access confidential information. Among the confidential items those prying eyes would like are: our contacts; intimate relationships and activities; political choices and preferences; government records, genetic, biometric, and health data (pre-birth to post-death); education and employment records; phone, text, and email correspondence; social media likes, friends, and preferences; browsing activity, location, and movement,; purchasing habits; banking, insurance, and other financial information; and data from our connected devices and wearables. We generate an enormous amount of data

---

[45] *Id.*
[46] *See* Daniel J. Solove & Neil M. Richards, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007).
[47] Micelle Finneran Dennedy et al., *The Privacy Engineer's Manifesto,* MCAFEE (2014), https://link.springer.com/content/pdf/10.1007%2F978-1-4302-6356-2.pdf.
[48] *Id.*
[49] Allen-Castellitto, *supra* note 44.

every day. Keeping it private is a herculean task. On the other hand, penetrating our defenses can be very easy and profitable.

Data not only defines us, it is the lifeblood of AI. Data science is the new discipline of the digital age. Companies like Facebook, Snapchat, or Google are not primarily in the social media or consumer tools business; rather they are in the data business. The products they offer (in most cases free to the end user) are vehicles to collect massive quantities of rich data, making the user essentially the product. The valuable commodity drives their business models and revenue streams.[50] Indeed, "personal data has become the most prized commodity of the digital age, traded on a vast scale by some of the most powerful companies in Silicon Valley and beyond."[51] The result is the datafication of society.

AI and its capacity to process vast amounts of data undermines privacy in many forms. In the following sections we detail some of the ways in which AI can compromise our privacy and free will. Some of the mechanisms discussed were developed before AI. However, AI can be deployed in all of them, making each more efficient and thus more of a threat. Indeed, we have already entered "the age of privacy nihilism."[52]

B. Data Collection, Analytics, and Use

Due to data's significance, technology companies will always push legal and ethical boundaries in pursuit of collecting more data to create models that make better and better predictions. Then they share this information with government agencies and private actors.

---

[50] *See, e.g.,* Damien Collins, *Summary of Key Issues from the Six4Three Files*, https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf (describing how Facebook traded access to user data in exchange for advertising buys).

[51] Gabriel J.X. Dance et al., *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html (describing how personal data was traded among 150 companies without user consent).

[52] Ian Bogost, *Welcome to the Age of Privacy Nihilism*, ATLANTIC (Aug. 23, 2018), https://www.theatlantic.com/technology/archive/2018/08/the-age-of-privacy-nihilism-is-here/568198.

There are inadequate legal protections to prevent these disclosures of information. Understanding the full picture that without data, a big part of modern AI cannot exist, puts data privacy and democracy at the epicenter of concern.

Data collectors or third party "cloud" storage services maintain the large-scale data collected by IoT, surveillance, and tracking systems in diverse databases. While in isolation, individual data sets dispersed across thousands of servers may provide limited information insights, this limitation can be resolved by a process known as "data fusion," which merges, organizes, and correlates those data points.[53] Once data is collected, synthesized, and analyzed, third parties create sophisticated profiles of their "data subjects"[54] that offer a trove of useful intelligence to anyone who wants to influence or manipulate purchasing choices and other decisions.

AI is the engine behind the data analytics. It enables predictive decision-making based on consumers' financial, demographic, ethnic, racial, health, social, and other data. For example, IBM's Watson provides Application Program Interfaces (APIs) that allow developers to create their own natural language interfaces.[55] Google's Tensor Flow is an open-source platform and library that similarly permits AI developers to harness the power of machine learning for numerous applications.[56] For its "Photo Review" program, Facebook developed "Deep Face," a deep learning facial recognition system that works by identifying "principal components" in a picture and

---

[53] *See* Sadia Din et. al, *A Cluster-Based Data Fusion Technique to Analyze Big Data in Wireless Multi-Sensor Systems,* IEEE ACCESS (Feb. 2, 2017), https://ieeexplore.ieee.org/document/7873266 (describing data fusion).
[54] Under the definition adopted by the EU in the General Data Protection Regulation, a data subject is "an identified or identifiable natural person" whose personal data is collected or processed. See Art. 4 (1) EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[55] *See* IBM, https://www.ibm.com/watson (last visited Aug 1, 2018).
[56] *See* Tensor Flow, https://www.tensorflow.org (last visited Aug. 1, 2018).

comparing those to a reference dataset.[57] Deep Face is more accurate than the FBI's comparable system.[58] Technological advances in AI's power and speed have enabled such systems to uncover more and more potentially relevant insights from extraordinarily sophisticated and complex data sets.

Developments in data collection, analytics, and use threaten privacy rights not explicitly protected by the four privacy torts codified in state law. Moreover, they have the potential to both benefit and harm society. For example, health data could be used for research to cure diseases but also to disqualify candidates for lower insurance premiums. The aggregation and coordination of disparate databases can reveal everything from buying habits to health status to religious, social, and political preferences. Courts have begun to recognize the threat this poses. In *United States v. Jones*, a majority of the Supreme Court signed on to or concurred in support of a "mosaic theory," under which long-term surveillance can be considered a search in violation of the Fourth Amendment because of the detailed picture aggregated location information provides.[59] As Justice Sotomayor's concurrence noted, the government's ability to store and mine this information for an indefinite duration "chills associational and expressive freedoms"[60] and undermines the checks and balances used to constrain law enforcement. If allowed, such unfettered discretion to track citizens could have detrimentally affected relations between the government and citizens in ways that threaten democracy.

AI exacerbates and exponentially multiplies the existing trends to over collect data and use data for unintended purposes not disclosed to users at the time of collection. Supervised machine learning requires large quantities of accurately labeled data to train algorithms. The more data the higher the quality of your learned algorithm will

---

[57] Gurpreet Kaur, Sukhvir Kaur & Amit Walia, *Face Recognition Using PCA, Deep Face Method*, 5 INT'L J. COMPUTER SCI. & MOBILE COMPUTING 359, 359-366 (2016).
[58] Russell Brandom, *Why Facebook is Beating the FBI at Facial Recognition*, VERGE (July 7, 2014), https://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition (97% accuracy for DeepFace vs. 85% for FBI systems).
[59] United States v. Jones, 565 U.S. 400 (2012).
[60] *Id.* at 416 (Sotomayor, J., concurring).

be. The more variables or features, the more complex and potentially accurate the model can be. Thus the companies that succeed will be the ones not with the best algorithm, but with access to the best data. The more data collected the smarter, faster and more accurate the algorithms will be. There is an incentive to over collect and use data to develop algorithms to accomplish novel tasks. The phrase "data is the new oil" has recently been coined to capture the idea that data is a valuable commodity that can be monetized.[61] Whoever has the best data in terms of quantity and quality, has the opportunity to create disruptive businesses models and revenue producing powerhouses.

1. The Internet of Things

The power behind artificial intelligence lies in a machine's access to data. That is essentially what AI does: it crunches data. Thus, the more points of information about a data subject or larger the accessible data set, the better capable AI will be of answering a query or carrying out a function.[62]

The Internet of Things ("IoT") is an ecosystem of electronic sensors found on our bodies, in our homes, offices, vehicles, and public places.[63] "Things" are any human-made object or natural object that is assigned an internet address and transfers data over a network without human-to-human or human-to-computer interaction."[64] If AI is like the human brain, then IoT is like the human body collecting sensory input (sound, sight, and touch).[65] IoT devices collect the raw data of people carrying out physical actions and communicating

---

[61] *The World's Most Valuable Resource Is No Longer Oil, but Data*, ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[62] *See generally* SAS, *Artificial Intelligence: What it is and Why it Matters,* SAS, https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html.

[63] *See* https://en.wikipedia.org/wiki/internet_of_things.

[64] Margaret Rouse, *Internet of Things*, TECH TARGET (July 2016), https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[65] Calum McClelland, *The Difference Between Artificial Intelligence, Machine Learning, and Deep Learning*, MEDIUM (Dec. 4, 2017), https://medium.com/iot-forall/the-difference-between-artificial-intelligence-machine-learning-and-deep-learning-3aa67bff5991.

with others.[66] Such devices have facilitated the collection, storage, and analysis of vast amounts of information.[67]

Cisco, the networking company, estimates there will be 50 billion new connected "things" by 2020, one trillion by 2022, and 45 trillion in twenty years.[68] Once those "things" collect our information, AI-based programs can use that data partly to enhance our lives, but also to influence or control us.[69] While IoT renders our every movement and desire transparent to data companies, the collection and use of our information remains opaque to us. The enormous information asymmetry creates significant power imbalances with privacy as the main casualty.

2. The Surveillance Ecosystem

"Things" are not the only data capture devices we encounter. They are accompanied by both physical and online surveillance systems. The ubiquity of such systems makes them seem harmless or at least familiar. Consider messaging platforms such as Microsoft's Skype, Tencent's WeChat, or Facebook's WhatsApp and Messenger. You pay for those free or low-cost services with your data.[70] Also consider communications systems: email, text messaging, telephone, cellular and IP voice telephony. As the old joke goes, your phone is now equipped with 3-way calling: you, the person you called, and the government. Add in communications providers that sniff your messages, log your metadata, and track your activities, and the scope of the problem becomes clear.

Visual methods also capture personal data including through advanced technologies such as aerial and satellite surveillance, drones,

---

[66] *Id*.
[67] *Id.*
[68] Vala Afshar, *Cisco: Enterprises are Leading the Internet of Things Innovation,* HUFFINGTON POST (Aug. 28, 2017), https://www.huffingtonpost.com/entry/cisco-enterprises-are-leading-the-internet-of-things_us_59a41fcee4b0a62d0987b0c6.
[69] *See* Helbing, *supra* note 6.
[70] *See* Samuel Gibbs *How Much Are You Worth to Facebook,* GUARDIAN (Jan. 28, 2016), https://www.theguardian.com/technology/2016/jan/28/how-much-are-you-worth-to-facebook.

license plate readers, street cameras, security cameras, infrared cameras, and other remote and enhanced imaging devices.[71] Google's "Sidewalk Labs" is building a "smart city," using "ubiquitous sensing" of all pedestrian and vehicular activity.[72]

There is no privacy on the internet. Here are a few reasons why. Small file "cookies" surreptitiously placed on a user's hard drive track his or her movement across the internet and deliver that information to servers.[73] User data collected by "spotlight ads," "web beacons" and "pixel tags" may include: the amount of time spent on each page, activity, page scrolls, referring web site, device type, and identity. While users can invoke the "Do Not Track" (DNT) setting on their browsers, there is no requirement that web sides honor DNT requests, so most ignore them.[74] Users may also attempt to employ other privacy-enhancing methods including virtual private networks, end-to-end encryption, and ad-blockers, but such methods will not always succeed.

The business model for social media and other "free" online services depends on the ability to "monetize" data and content.[75] Ultimately, the exercise that these companies need to embark on to exist is to find insights and predictions regarding user profiles, preferences, and behavior. These companies then sell and share the data for various purposes (e.g., advertising targeting and election tampering). This is a form of surveillance. And, because it is done not for public safety but to generate profits, it is called "surveillance capitalism."

---

[71] Robert Draper, *They Are Watching You – and Everything Else on the Planet*, NAT'L GEOGRAPHIC (Dec. 2017), https://www.nationalgeographic.com/magazine/2018/02/surveillance-watching-you.

[72] Sidney Fussell, *The City of the Future Is a Data-Collection Machine*, ATLANTIC (Nov. 21, 2018), https://www.theatlantic.com/technology/archive/2018/11/google-sidewalk-labs/575551.

[73] Joanna Geary, *Tracking the trackers: What are Cookies? An Introduction to Web Tracking*, GUARDIAN (Apr. 23, 2012), https://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro.

[74] *See generally* Jon Brodkin, *Websites Can Keep Ignoring "Do Not Track" Requests After FCC Ruling*, ARS TECHNICA (Nov. 6, 2015), https://arstechnica.com/information-technology/2015/11/fcc-wont-force-websites-to-honor-do-not-track-requests.

[75] The data marketplace is estimated to represent $150 to $200 billion dollars annually.

It is an ecosystem fueled by data extraction rather than the production of goods.[76]

The market capitalization of the major tech companies reveals just how much their users and their data are worth to them. As of August 2018, Apple was worth $1 trillion;[77] Amazon $890 billion; Alphabet (Google's parent company) $861 billion; and Facebook $513 billion. Collectively, the FAANG giants (Facebook, Amazon, Apple, Netflix and Google) have a net worth of $3.5 trillion, roughly equal to the GDP of Germany, the world's fourth largest economy.[78] Profit as they do off of our data, the acronym is apt.

On July 26, 2018, the stock price of Facebook fell by 20%, shedding over $100 billion in capitalized value, the largest one-day drop in stock market history.[79] Many analysts attribute this fall to Facebook's implementation of new European privacy rules and attendant pull back in the sale of user data.[80] The following day Twitter's stock price also fell by 20% for the same reason.[81] These events demonstrate that greater privacy protections may hurt companies stocks prices in some instances.

Illegal means of collecting private information are even more effective than legal ones. These include cyber intrusion by viruses, worms, Trojan horses, keystroke logging, brute-force hacking and other attacks.[82] While AI is often deployed to help make data safe,

---

[76] Shoshana Zuboff, *Google as Fortune Teller, The Secrets of Surveillance Capitalism*, PUB. PURPOSE (Mar. 5, 2016), https://publicpurpose.com.au/wp-content/uploads/2016/04/Surveillance-capitalism-Shuboff-March-2016.pdf.
[77] Market capitalizations for listed companies can be found at many financial sites, such as https://ycharts.com/companies.
[78] *See, e.g.,* https://www.investopedia.com/insights/worlds-top-economies.
[79] Akane Otani and Deepa Seetharaman, *Facebook Suffers Worst-Ever Drop in Market Value,* WALL ST. J. (July 26, 2018), https://www.wsj.com/articles/facebook-shares-tumble-at-open-1532612135.
[80] *See* Emily Stewart, *The $120-Billion Reason We Can't Expect Facebook To Police Itself*, VOX (July 28, 2018), https://www.vox.com/business-and-finance/2018/7/28/17625218/facebook-stock-price-twitter-earnings.
[81] *Id.*
[82] *See Cyber Threat Basics, Types of Threats, Intelligence & Best Practices,* SECUREWORKS (May 12, 2017), https://www.secureworks.com/blog/cyber-threat-basics.

more often it helps hackers get through defenses.[83] AI also turns the raw data collected by IoT and surveillance systems into meaningful intelligence that can be used by data companies for legal or pernicious purposes.[84]

3. Government Surveillance

The federal government has mastered the art of ubiquitous surveillance, some legal and some illegal. Rather than survey the copious types of surveillance, and Supreme Court cases upholding or rejecting them, here we discuss only those forms and doctrines that contribute to AI's erosion of privacy interests. We start with the third-party doctrine, which essentially holds that the Fourth Amendment does not apply when the government obtains data about a subject indirectly from a "third-party," rather than directly from the subject.[85] A classic case is the proverbial jailhouse informant who, having obtained information from a suspect, can freely provide that information to the prosecutor over the defendant's objection. But the doctrine goes farther. Anyone who discloses otherwise protected information to a third-party has, perhaps, "misplaced trust" in that person and loses any expectation of privacy she might otherwise have.

The misplaced trust and third-party doctrines mean that, absent statutory or common-law restrictions, government may obtain information about you from anyone who has it.[86] Third parties and the data they possess include everything travel companies and GPS enabled applications (such as Waze and Google Maps), which collect travel histories and searches, to financial service entities (such as

---

[83] Olivia Beavers, *Security Firm Predicts Hackers Will Increasingly Use AI to Help Evade Detection in 2019*, HILL (Nov. 29, 2018), https://thehill.com/policy/cybersecurity/418972-security-firm-predicts-hackers-will-increasingly-use-ai-to-help-evade.

[84] *See* McClelland, *supra* note 65.

[85] Smith v. Maryland, 442 U.S. 735, 743-44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties").

[86] If the third-party is another state actor who has obtained information in violation of the Fourth Amendment, then its ultimate use would also be impermissible.

banks and credit companies), which have customers' financial information, to medical care providers and insurers, which possess patient medical records.

Indeed, there is little information that some third-party does not already have or have access to. There are some federal statutory protections such as the Health Insurance Portability and Accountability Act (HIPAA), [87] the Electronic Communications Privacy Act (ECPA)[88] and the Fair Credit Reporting Act (FCRA).[89] But these cover only a small fraction of entities. Privacy obligation for most others stem either from contract (Terms of Use agreements), state law, or a common-law fiduciary relationship. Most of those rules make exceptions for law enforcement or judicial requests for records.

4. Anonymity

While informational privacy is concerned with concealing our activities from others, anonymity allows us to disclose our activities but conceal our identities. It enables participation in the public sphere that might be avoided if associations were known.[90] In *McIntyre v. Ohio Elections Commission*, the Supreme Court stated,"Anonymity is a shield from the tyranny of the majority. . . It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society." [91]

A famous *New Yorker* cartoon shows a dog browsing the internet and saying to a fellow canine: "On the Internet, nobody knows

---

[87] 42 U.S.C. 201. Most HIPAA requirements were promulgated by regulation by the Department of Health and Human Services. See 45 CFR 160.100, et seq.
[88] 18 U.S.C. 2510, et seq. ECPA applies to transient communications (Title I), stored communications (Title II) and addressing information (Title III). Public and private entities are subject to ECPA.
[89] 15 U.S.C. 1681, et seq.
[90] Bradley Smith, *What Hamilton Teaches Us About the Importance of Anonymous Speech*, WASH. POST (Nov. 8, 2016), https://www.washingtonpost.com/opinions/what-hamilton-teaches-us-about-the-importance-of-anonymous-speech/2016/11/08/dd17ae3c-a53d-11e6-8fc0-7be8f848c492_story.html.
[91] 514 U.S. 334, 357 (1995).

you're a dog."[92] That may have been true before AI, when cross-referencing IP addresses with other data was cumbersome. Now, however, things aren't so simple.

Anonymization is the process of stripping personally identifiable information from collected data so the original source cannot be identified.[93] A related process, pseudonymization, replaces most identifying data elements with artificial identifiers or pseudonyms.[94] It involves techniques like hashing, data masking or encryption which reduce the likability of datasets with the individual's identifying information.[95] The current legal distinction is pseudonymized data can be re-identified (e.g., reconnecting the individual to their information).[96] However, the law fails to consider AI's ability to re-identify anonymized data.[97]

AI is great at re-identifying (or de-identified) data by extracting relationships from seemingly unrelated data. A University of Melbourne study was able to re-identify some Australian patients surveyed through their supposedly anonymous medical billing records.[98] Similar results are available with credit card metadata.[99] Af-

---

[92] Peter Steiner, The New Yorker, July 5, 1993.
[93] *See* https://en.wikipedia.org/wiki/Data_anonymization.
[94] Clyde Williamson, *Pseudonymization vs. Anonymization and How They Help With GDPR*, PROTEGRITY (Jan. 5, 2017), https://www.protegrity.com/pseudonymization-vs-anonymization-help-gdpr.
[95] Id.
[96] *Data Masking: Anonymization or Pseudonymization?*, GDPR REPORT (Sept. 28, 2017), https://gdpr.report/news/2017/09/28/data-masking-anonymization-pseudonymization.
[97] Boris Lubarsky, *Re-Identification of "Anonymized Data"*, 1 GEO. L. TECH. REV. 202, 208-11 (2017).
[98] *See* Cameron Abbott et al., *De-identification of Data and Privacy*, K&L GATES (Feb. 26, 2018), http://www.klgates.com/de-identification-of-data-and-privacy-02-26-2018. *See also* Liangyuan Na et al., *Feasibility Of Reidentifying Individuals In Large National Physical Activity Data Sets From Which Protected Health Information Has Been Removed With Use Of Machine Learning*, JAMA NETWORK OPEN (Dec. 21, 2018), https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2719130 (95% reidentification accuracy based on data collected from smart watches, smartphones and fitness trackers).
[99] Yves-Alelexandre de Montjoye et al., *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata,* 347 SCI. 536 (Jan. 30, 2015),

ter the entire New York Taxi dataset for 2014 was disclosed, a researcher was able to identify celebrities entering taxicabs, their "pick up location, drop off location, amount paid, and even amount tipped."[100]

Thus with AI, the notion of anonymity in the public sphere is an illusion at best, however regulations continue to function based on this illusion. The "erosion of anonymity" lead the President's Council of Advisors on Science and Technology in 2014 to call for a wholesale reevaluation of privacy protections.[101] That has not happened yet. The lack of regulatory urgency to address technical changes and the lack of protection of privacy demonstrates a degradation of trusted democratic legal frameworks.

C. Decisional Privacy (Autonomy)

Autonomy comes from the Greek *autos* (self) and *nomos* (rule). As used by the Greeks, the term meant political autonomy.[102] But its centrality to democracy now extends to other aspects of autonomy including the right to make decisions about oneself and one's life trajectories, which we call "decisional privacy."[103] As understood today, autonomy refers to "a set of diverse notions including self-governance, liberty rights, privacy, individual choice, liberty to follow one's will, causing one's own behavior, and being one's own

---

http://science.sciencemag.org/content/347/6221/536 ("even data sets that provide coarse information at any or all of the dimensions provide little anonymity and that women are more reidentifiable than men in credit card metadata").

[100] Boris Lubarsky, *Re-Identification of "Anonymized" Data*, 1 GEO. L. TECH. REV. 202, 211 (2017).

[101] President's Council of Advisors on Science and Technology, *Report to the President Big Data and Privacy: A Technological Perspective,* PCAST (May 2014), at 22, https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf.

[102] *Autonomy*, MERRIAM-WEBSTER DICTIONARY ONLINE, https://www.merriam-webster.com/dictionary/autonomy (last visited April 22, 2019).

[103] *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965) (finding "a right to privacy in the 'penumbras' and 'emanations' of other constitutional protections.").

person."[104] Autonomy is highly correlated with free will and is essential to human dignity and individuality.

The upshot of this is that autonomy *qua* freedom of choice is important both in terms of human development and law. Those hoping to influence the actions of others (let's call them "influencers") often tread too closely to the line separating persuasion from coercion.

1. Subverting Free Will – Online Behavioral Advertising

The advertising industry is expert at influencing people's habits and decisions. Madison Avenue has been practicing the art of persuasion as long as there have been advertiser-supported media. Conventional advertising can be annoying but seldom raises the concerns discussed here. However, in the digital era, a special type of influence has emerged known as "online behavioral advertising." Here, third-party advertising technology companies use AI to tailor advertisements to target particular users for particular contexts.[105] The third parties sit in between the publishing website or app and the advertiser that buys ad space on a website. These third parties need massive amounts of data for this technique to work. Not only do companies deploy personal information for private benefit, they often do so covertly. While this is ostensibly done to "inform" our choices, it can easily become subtle but effective manipulation. When that occurs, behavioral advertising compromises decisional privacy as well as informational privacy and erodes foundational democratic principles of free will, equality, and fairness.

Online behavioral advertising, and marketing delivers benefits as well as costs. On the plus side, it can reduce search costs for consumers and placement costs for vendors. It is also the backbone of the "internet" economy since ad revenue supports services that would not otherwise be free. But behavioral advertising also has downsides. First, personal data must be collected to make the system work. The resulting loss of privacy was explored above. Second and more pernicious is the ability to acutely manipulate consumer

---

[104] TOM L. BEAUCHAMP & JAMES F. CHILDRESS, PRINCIPLES OF BIOMEDICAL ETHICS 67-68 (1989).
[105] *See generally* Steven C. Bennett, *Regulating Online Behavioral Advertising*, 44 J. MARSHALL L. REV. 899 (2011).

choice. As the information about each of us becomes more granular and complete, behavioral advertising can create psychological "wants" that masquerade as cognitive choices. Users only defense mechanism is to opt-out under the mistaken belief that this stops their data from being used or collected.[106] There is a continuum of influence from persuasion to manipulation to coercion. Philosophers and autonomy theorists debate where the boundaries are, but most agree that influence can devolve into coercion.[107]

The Federal Trade Commission (FTC) has issued "principles" and guidelines but no binding regulations regarding the use of online behavioral advertising.[108] It takes mostly a hands-off approach except in extreme cases of companies engaging in unfair or deceptive business practices.[109] Although Congress has held hearings,[110] it too has failed to regulate these practices. Some states have attempted to fill the void, but such laws have questionable effect and constitutionality given the borderless nature of the internet. Thus, we are left with industry self-regulation, which often means little or no constraints at all.

2. Consumer Acquiescence

Much of the data collection and use practices are widely known to technology aficionados yet persists through consumer acquiescence and regulatory forbearance. Today, people reveal much more information to third parties than before. Some may tradeoff privacy for

---

[106] While opting-out may abate personalized ads, it does not stop advertisers from generic advertising, data collection, use, sharing and retention practices.
[107] *See* Trent J. Thornley, *The Caring Influence: Beyond Autonomy as the Foundation of Undue Influence*, 71 IND. L.J. 513, 524 (1996).
[108] *See, e.g.*, FTC, *Self-Regulatory Principles for Online Behavioral Advertising*, FTC Online Tracking Guidance (2016), www.ftc.gov/os/2009/02/P085400behavioralreport.pdf.
[109] *See* Federal Trade Commission Act, 15 U.S.C. §§ 45. The FTC will also police the collection of information that is protected by statute, such as medical and financial information.
[110] *Behavioral Advertising: Industry Practices and Consumers' Expectations: Joint Hearing Before the H. Comms. On Commerce, Trade, and Consumer Protection and on Communications, Technology, and the Internet*, 111th Cong. (2009); *Privacy Implications of Online Advertising: Hearing Before the S. Comm. on Commerce, Science, and Transportation, 110th Cong.* (2008).

worthwhile convenience or merely accept this "diminution of privacy as inevitable."[111] After all, people are getting free or convenient services, reduced search and transaction costs, and otherwise benefiting from advanced technology and the IoT. However, Justice Sotomayor suggested in her concurrence in *Jones* that she seriously doubts people will accept it as inevitable.[112] The benefits one gets are not free or cheap. People pay with their private personal information. Users in North America are worth over $1,000 each to Facebook.[113] Google profits with each "free" search you perform on their platform.

Increasing consumer awareness of the privacy invasions resulting from online tracking and data collection – particularly after the Cambridge Analytica scandal – has created a "creepiness factor" in the use of the internet and connected devices. IBM conducted a survey that found 78 percent of consumers in the United States believe a technology company's ability to safeguard its data is "extremely important."[114] However, only 20 percent of consumers "completely trust" the companies to protect data about them.[115] In another survey conducted by Blue Fountain Media, 90 percent of participants were very concerned about privacy on the internet,[116] but at the same time, 60 percent happily downloaded apps without reading the terms of use.[117]

These surveys show that consumers care about privacy, but do not feel empowered to take control of their data or think they have the

---

[111] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).
[112] *Id*.
[113] Facebook revenue in 2016 was $13.54 per quarter per user or $54.16 per year. At a 3% capitalization rate, that equals $1,805. *See* Gibbs, *supra* note 70; PCAST, *supra* note 101. Similarly, users "derive over $1000 of value annually on average from Facebook" and other communication technologies. Jay R. Corrigan, et al, *How Much Is Social Media Worth? Estimating The Value Of Facebook By Paying Users To Stop Using It*, https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0207101.
[114] IBM, *New Survey Finds Deep Consumer Anxiety over Data Privacy and Security,* PR NEWSWIRE (Apr. 16, 2018 12:01 PM), https://www.prnewswire.com/news-releases/new-survey-finds-deep-consumer-anxiety-over-data-privacy-and-security-300630067.html.
[115] *Id.*
[116] Ian Barker, *Consumers' Privacy Concerns Not Backed by Their Actions,* BETANEWS (June 2018), https://betanews.com/2018/05/31/consumer-privacy-concerns.
[117] *Id.*

rights to enforce privacy protections. These beliefs are not misplaced. Most if not all tech companies do not negotiate terms of use or privacy policies with consumers that do not agree to them; rather if you don't agree to data collection and use, then you cannot use the service.

So long as powerful forces endeavor to control what should be autonomous decisions, privacy will continue to erode. Artificial intelligence creates opportunities and capabilities to further erode human autonomy. It builds on the successes of "surveillance capitalism" to manipulate our consumption and life choices. In the next section we discuss how political actors employ AI and the techniques of behavioral advertising to manipulate voters and influence elections.

III. THREATS TO ELECTIONS AND DEMOCRATIC INSTITUTIONS

Modern democracies have come to stand for a commitment to a set of core principles including political discourse, civil rights, due process, equality, economic freedoms, and the rule of law. Artificial intelligence challenges these core tenants in several ways. First and foremost is the use of "weaponized AI" to disrupt and corrupt democratic elections. This can be done through physical means such as cyberattacks and through psychological means by poisoning people's faith in the electoral process. Second, malevolent actors can use AI to weaken democratic institutions by undermining a free press and organs of civil society. A third and in some sense the most pernicious impact of AI is its effect on our core values of equality, due process, and economic freedom. Here, no motive needs to be ascribed. By structure alone AI resists three of democracy's main features: transparency, accountability, and fairness. We have misplaced trust in the perceived "neutrality" and competence of machines, when in fact they can exacerbate human biases and flaws.

In this section we describe the threats AI poses to core democratic values and institutions and to democracy itself.

A. Self-Governance and Political Participation

Free and open elections are the bedrock of American democracy. But as recent events have made painfully clear, elections can be

hacked. By that we mean more than just cyberattacks where vulnerable voting systems are penetrated by "malign foreign actors,"[118] although that surely occurs and remains a major threat.[119] Rather, we mean the full array of efforts to subvert or burden fair and free elections. AI can both contribute to the effectiveness of existing efforts to distort voting, for example by facilitating the drawing of gerrymandered districts,[120] as well as create new opportunities for election interference.

We describe several different kinds of cyberthreats to the electoral process. First, are the traditional types of cyber intrusions where actors gain access to computer systems and steal or corrupt confidential election information. A second and more potent form of hacking is the manipulation of voter attitudes through weaponized "microtargeted" propaganda. The techniques used are similar to the hijacking of consumer choices discussed above.[121] We next discuss fake news, which is a vital and potent ingredient of voter manipulation. Finally, we show how anti-democratic forces endeavor to sow doubt in trusted institutions as a means of conditioning voters to accept extreme views. In each of these methods, artificial intelligence can be used both to increase effectiveness and to mask the purposes and methods of voter suppression and manipulation.

1. Hacking the Vote – Cyberthreats to Elections

It is now undisputed that Russian intelligence operatives interfered in the 2016 election in the United States and continue to target U.S. electoral systems.[122] They attempted to penetrate election software

---

[118] Eric Geller, *Despite Trump's Assurances, States Struggling to Protect 2020 Election*, POLITICO (July 27, 2018), https://www.politico.com/story/2018/07/27/trump-election-security-2020-states-714777.
[119] *See* Andrew Gumbel, *Why US Elections Remain "Dangerously Vulnerable" to Cyberattacks*, GUARDIAN (Aug. 13, 2018), https://www.theguardian.com/us-news/2018/aug/13/us-election-cybersecurity-hacking-voting.
[120] Daniel Oberhaus, *Algorithms Supercharged Gerrymandering. We Should Use Them to Fix it*, VICE (Oct. 3, 2017), https://motherboard.vice.com/en_ us/article/7xkmag/gerrymandering-algorithms.
[121] *See supra* Section III.C.
[122] While this article was in final edits, the Department of Justice released a redacted version of Special Counsel Robert Mueller's *Report on the Investigation Into Russian Interference in the 2016 Presidential Election* or "Mueller Re-

and equipment in at least twenty-one states, launched cyberattacks against a voting software company, hacked into the emails of one-hundred local election officials,[123] and accessed at least one campaign finance database.[124] However they relied principally on leaks of the data obtained from cyber operations including penetration of the servers of the Democratic National Committee and the email account of Clinton campaign chairman John Podesta.[125]

The Obama administration was so concerned about Russian hacking during the 2016 election that it developed a contingency plan to "send[] armed federal law enforcement agents to polling places, mobilizing components of the military and launching counter-propaganda efforts."[126] "The plan reflects how thoroughly the Russian effort to undermine public confidence in the U.S. electoral system had succeeded."[127] A Gallup poll bore this out. "A record-low of 30% of Americans expressed confidence in the `honesty of elections.'"[128]

---

port"). *See* Roberrt S. Mueller, III, *Report on the Investigation Into Russian Interference in the 2016 Presidential Election* (March 2019), https://www.justice.gov/storage/report.pdf. A searchable version is available at *Read the Muller Report*, N.Y. TIMES (April 18, 2019), https://www.nytimes.com/interactive/2019/04/18/us/politics/mueller-report-document.html. The report confirms many of the findings previously made about Russian interference in the election. *Id.* at 14-50. *See also* Nat'l Intelligence Council, *Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections*, Jan. 6, 2017, at 2, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[123] *See, e.g.*, Mueller Report, *supra*, note 122 at 51 (describing spearphishing attacks on Florida election officials).

[124] *National Defense Authorization Act for Fiscal Year 2018: Hearing on H.R. 5515*, 115th Cong. (2017) (remarks of Sen. Klobuchar); *Bolstering the Government's Cybersecurity: Lessons Learned from Wannacry: Joint Hearing Before the H. Comm. on Oversight and on Research and Technology*, 115th Cong. (2017), https://www.govinfo.gov/content/pkg/CHRG-115hhrg26234/pdf/CHRG-115hhrg26234.pdf.

[125] *Id.*

[126] Massimo Calabresi, *Exclusive: Read the Previously Undisclosed Plan to Counter Russian Hacking on Election Day*, TIME (July 20, 2017), http://time.com/4865798/russia-hacking-election-day-obama-plan.

[127] *Id.*

[128] Gallup, *Update: Americans' Confidence in Voting, Election*, GALLUP (Nov. 1, 2016), https://news.gallup.com/poll/196976/update-americans-confidence-voting-election.aspx.

Election hacking is not a new phenomenon, but it has been exacerbated by AI. U.S. officials and researchers have been concerned for decades about the vulnerability of state and local election machinery, especially voting devices that do not produce a paper trail.[129] What is different now is the increasing use of artificial intelligence to improve cyberattacks. New heuristics, better analytics, and automation are now key to successful attacks. AI "is helping hackers attack election systems faster than officials can keep up."[130]

Cyberattackers were early adopters of AI. By using machine learning to analyze vast amounts of purloined data, they can more effectively target victims and develop strategies to defeat cyber defenses.[131] Indeed in its 2018 AI Predictions report, the consulting firm Price Waterhouse Coopers describes "one job where AI has already shown superiority over human beings [-] hacking."[132] While most cybercrimes are financial, cyber intrusions are increasingly being used for espionage and military purposes. In addition, cyberattacks and malware can be deployed to advance political, ideological, and other strategic objectives. If the objective is to undermine democratic participation, AI is an indispensable tool.

The good news, however, is that AI can be used defensively as well as offensively.[133] For example, the winner of the Department of Defense's DARPA Cyber Grand Challenge used AI deep learning to

---

[129] *See Verification, Security and Paper Records for Our Nation's Electronic Voting Systems: Hearing Before the H. Comm on House Administration*, 109th Cong. (2006), https://www.govinfo.gov/content/pkg/CHRG-109hhrg31270/pdf/CHRG-109hhrg31270.pdf. *See generally* Eric Manpearl, *Securing U.S. Election Systems: Designating U.S. Election Systems as Critical Infrastructure and Instituting Election Security Reforms*, 24 B.U. J. SCI. & TECH. L. 168 (2018).

[130] Dan Patterson, *How AI is Creating New Threats to Election Security*, CBS NEWS (Nov. 6, 2018, 11:50 AM), https://www.cbsnews.com/news/how-ai-will-shape-the-future-of-election-security.

[131] Kevin Townsend, *How Machine Learning Will Help Attackers*, SECURITY WEEK (Nov. 29, 2016), https://www.securityweek.com/how-machine-learning-will-help-attackers.

[132] PWC, *AI predictions for 2018*, at 14, https://www.pwc.com/us/en/advisory-services/assets/ai-predictions-2018-report.pdf (last visited Aug. 1, 2018).

[133] *See generally The Promises and Perils of Emerging Technologies for Cybersecurity: Hearing Before the Senate Committee on Commerce, Science and Transportation*, 115th Cong. (2017).

defeat cyberattacks.[134] The bad news is that resources deployed at each end of this cyberwar are asymmetric, especially with state-sponsored cyberattacks. , While our adversaries are ramping up AI research funding,[135] the United States is cutting it. We are even disinclined to upgrade our election machinery to better resist cyberattacks.[136] In some ways, "we are a 20th century analog system … operating on DOS."[137]

2. Hacking the Mind – Psychographic Profiling and Other Influencers

In addition to specific cyberattacks, the Russian government also conducted an influence campaign that sought to undermine public trust in democratic institutions and elections.[138] This type of interference relies heavily on AI capabilities. For example, on the day before Wikileaks released its first installment of the stolen emails from John Podesta, Russian disinformation operatives blasted 18,000 tweets to American voters. They were part of a highly adaptive AI operation involving 3,841 accounts controlled by the Russian Internet Research Agency that generated millions of pieces of fake news to shape the political narrative.[139] Such efforts are likely

---

[134] *See DARPA Celebrates Cyber Grand Challenge Winners*, DEF. ADVANCED RES. PROJECTS AGENCY (Aug. 5, 2016), https://www.darpa.mil/news-events/2016-08-05a.

[135] PWC Report, *supra* note 132, at 19-20.

[136] *See* Erin Kelly, *Bills To Protect U.S. Elections from Foreign Meddling Are Struggling, Senators Say,* USA TODAY (June 12, 2018), https://www.usatoday.com/story/news/politics/2018/06/12/bills-protect-elections-foreign-meddling-struggling/694385002 (referencing the bi-partisan Secure Elections Act, S.2261, https://www.congress.gov/bill/115th-congress/senate-bill/2261).

[137] *Sanctions and Financial Pressure: Major National Security Tools: Hearing Before H. Comm. on Foreign Affairs*, 115th Cong. 69 (2018) (remarks of Mr. Zarate and Mr. Yoho). DOS, or Disk Operating System, was the OS for the first IBM desktop computers in the 1980s.

[138] *See* Mueller Report, *supra* note 122, at 9.

[139] *See United States v. Internet Research Agency, et al.*, No. 18-cr-32 (D.D.C.), https://www.justice.gov/file/1035477/download; Craig Timberg & Shane Harris, *Russian Operatives Blasted 18,000 Tweets Ahead of a Huge News Day During the 2016 Presidential Campaign. Did They Know What Was Coming?*, WASH. POST (July 20, 2018), https://www.washingtonpost.com/technology/2018/07/20/russian-operatives-blasted-tweets-ahead-huge-news-day-during-presidential-campaign-did-they-know-what-was-coming.

to continue. A report by the Office of Director of National Intelligence concludes that "Russian intelligence services will continue to develop capabilities to provide Putin with options" to meddle in future elections.[140] The World Economic Forum was told in August 2017, that artificial intelligence has already "silently [taken] over democracy" through the use of behavioral advertising, social media manipulation, bots and trolls.[141]

Not all uses of data analytics in politics distort the process. Most campaigns now rely on data-focused systems and sophisticated algorithms for voter outreach and messaging.[142] However, there is a difference between legitimate and illegitimate uses of data and algorithms. In the former, data usage is mostly overt and traceable. The data itself is public, lawfully obtained, and at least partly anonymized. In the latter, the data is often ill-gotten and its usage is covert and designed to be unattributable.[143] Additionally, data fusion and analytics reveal deeply personal and granular detail about each "data subject," which is then used to micro-target and emotionally influence what should be a deliberative, private, and thoughtful choice. This process of psychometric profiling uses quantitative instruments to manipulate behaviors.[144] Free will is the obstacle here, which AI can help overcome.

---

[140] ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE 5 (2017)

[141] Vyacheslav Polonski, *How Artificial Intelligence Silently Took Over Democracy*, WORLD ECON. FORUM (Aug. 9, 2017), https://www.weforum.org/agenda/2017/08/artificial-intelligence-can-save-democracy-unless-it-destroys-it-first; *see also* Chris Meserole and Alina Polyakova, *The West Is Ill-Prepared for the Wave of Deep Fakes' That Artificial Intelligence Could Unleash*, BROOKINGS (May 25, 2018), https://www.brookings.edu/blog/order-from-chaos/2018/05/25/the-west-is-ill-prepared-for-the-wave-of-deep-fakes-that-artificial-intelligence-could-unleash.

[142] *See* Anne Applebaum, *Did Putin Share Stolen Election Data with Trump?*, WASH. POST (July 20, 2018), https://www.washingtonpost.com/opinions/global-opinions/did-putin-share-stolen-election-data-with-trump/2018/07/20/50854cc8-8c30-11e8-a345-a1bf7847b375_story.html.

[143] Emma Graham-Harrison & Carole Cadwalladr, *Cambridge Analytica Execs Boast of Role in Getting Donald Trump Elected*, GUARDIAN (Mar. 21, 2018), https://www.theguardian.com/uk-news/2018/mar/20/cambridge-analytica-execs-boast-of-role-in-getting-trump-elected.

[144] *See Meet Cambridge Analytica: The Big Data Communications Company Responsible for Trump & Brexit*, NONE ABOVE UK (Feb. 2, 2017), https://nota-

The data science firm Cambridge Analytica is the poster child for inappropriate use of data. It created psychographic profiles of 230 million Americans and repurposed Facebook to conduct psychological, political warfare.[145] Cambridge Analytica was co-founded by Steve Bannon, former executive editor of Breitbart and Donald Trump's first chief of staff. It was only natural that Jared Kushner would hire them to run Mr. Trump's digital campaign. However, Cambridge Analytica was no ordinary political consulting firm. It was built on the work of Prof. Aleksandr Kogan and graduate students at Cambridge University[146] who harvested 87 million American Facebook users' data without their consent.[147] One tool they used was a personality quiz that scored participants according to the "Big Five" metrics: openness, conscientiousness, extraversion, agreeableness and neuroticism.[148] Then, using AI, they leveraged these results with other data (up to 5,000 data points on each user) to reveal personality traits, emotions, political preferences and behavioral propensities.[149] The resulting "psychographic profiles" created from the data were then used by the firm to promote Trump's candidacy and by the campaigns of Republicans Ben Carson and Ted Cruz. .[150] They targeted respective audiences with up to 50,000 pinpoint ad variants each day leading up to the election. Alexander

---

uk.org/2017/02/02/meet-cambridge-analytica-the-big-data-communications-company-responsible-for-trump-brexit.

[145] *Id*.; Carole Cadwalladr, *'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower,* GUARDIAN (Mar. 18, 2018), https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

[146] Principal researchers included Michal Kosinski, David Stillwell and Christopher Wylie.

[147] *See* Issie Lapowsky, *The Man Who Saw the Dangers of Cambridge Analytica Years Ago*, WIRED (June 19, 2018), https://www.wired.com/story/the-man-who-saw-the-dangers-of-cambridge-analytica.

[148] *See* Cadwalladr *supra* note 145.

[149] Most of this was done in secret, except that a dataset was accidently left on GitHub, a code-sharing website, leading to its ultimate disclosure. Phee Waterfield & Timothy Revell, *Huge New Facebook Data Leak Exposed Intimate Details of 3m Users*, NEW SCIENTIST (May 14, 2018), https://www.newscientist.com/article/2168713-huge-new-facebook-data-leak-exposed-intimate-details-of-3m-users.

[150] David A. Graham, *Not Even Cambridge Analytica Believed It's Hype,* ATLANTIC (Mar. 20, 2018), https://www.theatlantic.com/politics/archive/2018/03/cambridge-analyticas-self-own/556016.

Nix, Cambridge Analytica CEO, boasted "he had put Trump in the White House."[151]

Micro-targeting with AI poses a challenge to election regulation. Big data analytics make distortion campaigns more successful, and thus more likely to be deployed, usually by unknown sources.[152] Election law depends to a large degree on transparency, both in funding and electioneering. Yet, spending on covert social media influence campaigns is not reported and often untraceable, such that foreign and illegal interferences go unregulated and undetected. While false campaign statements are apparently protected by the First Amendment,[153] having them exposed to sunshine, with real speakers' real identities tied to public scrutiny, imposes some discipline. That is lacking with covert influence campaigns. Their "willingness to flout the political honour code to undermine the legitimacy of our democratic institutions illustrates perfectly why a robust election regulation … is a critical component of a functioning democracy."[154]

In his article *Engineering an Election: Digital Gerrymandering Poses a Threat to Democracy*, Jonathan Zittrain describes an experiment in "digital gerrymandering" conducted by Facebook in 2010.[155] Facebook users were selectively shown news of their friends who had voted that day.[156] This increased turnout by prompting those who received the news to vote in sufficiently

---

[151] Nick Miller, *Cambridge Analytica CEO Suspended After Boasts of `Putting Trump in the White House*, SYDNEY MORNING HERALD (Mar. 21, 2018), https://www.smh.com.au/world/europe/cambridge-analytica-ceo-suspended-after-boasts-of-putting-trump-in-white-house-20180321-p4z5dg.html.

[152] *See* Vyacheslav Polonski, *How Artificial Intelligence Conquered Democracy*, CONVERSATION (Aug. 8, 2017, 6:33 AM), https://theconversation.com/how-artificial-intelligence-conquered-democracy-77675.

[153] *Cf.* United States v. Alvarez, 567 U.S. 709 (2012) (false statements not necessarily deprived of First Amendment protection); Susan B. Anthony List v. Dreihaus, 134 S.Ct. 2334 (2014) (resolving standing issue with false campaign speech).

[154] Observer Editorial, *The Observer View on Digital Campaigning Being an Existential Threat to Democracy*, GUARDIAN (July 29, 2018), https://www.theguardian.com/commentisfree/2018/jul/29/the-observer-view-on-digital-campaigning-threat-to-democracy.

[155] Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335 (2014).

[156] *Id*. at 335-36.

greater numbers that it could hypothetically affect election results.[157] Secret social media "recommendation algorithms" produce similar distortions.[158] "[T]he selective presentation of information by an intermediary to meet its agenda rather than to serve its users … represents an abuse of a powerful platform [and] is simply one point on an emerging map [of the ability] to quietly tilt[] an election."[159] Zittrain's next article was more emphatic; *Facebook could decide an election without anyone ever finding out*.[160]

Social media manipulation likely played a role in the 2016 U.S. election.[161] But we were not alone. A 2018 report by the Computational Propaganda Research Project found evidence of manipulation campaigns in 48 countries, where "at least one political party or government agency us[ed] social media to manipulate public opinion domestically."[162] This is big business. "Since 2010, political parties and governments have spent more than half a billion dollars on the research, development, and implementation of psychological operations and public opinion manipulation over social media."[163] To the same effect is the influencing of voters through the manipulation of search engine results.[164]

---

[157] *Id*. at 336.
[158] Paul Lewis, *Fiction Is Outperforming Reality: How YouTube's Algorithm Distorts Truth*, GUARDIAN (Feb. 2, 2018), https://www.theguardian.com/technology/2018/feb/02/how-youtubes-algorithm-distorts-truth.
[159] Zittrain, *supra* note 155 at 338.
[160] Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering.
[161] *See* Mueller Report, *supra* note 122 at 174.
[162] Samantha Bradshaw & Philip N. Howard, Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation 3 (2018). *See also* Tania Menai, *Why Fake News on WhatsApp Is So Pernicious in Brazil*, Slate (Oct. 31, 2018, 3:44 PM), https://slate.com/technology/2018/10/brazil-bolsonaro-whatsapp-fake-news-platform.html (reporting that newly elected Brazilian President Jair Bolsonaro profited from a massive disinformation campaign on WhatsApp, despite Facebook's deployment of a "war room" to abate the practice).
[163] Bradshaw, *supra* note 162, at 3.
[164] Robert Epstein et al., *Suppressing the Search Engine Manipulation Effect (SEME)*, https://cbw.sh/static/pdf/epstein-2017-pacmhci.pdf (last visited Feb. 18, 2019).

Election meddling "was not a one-time event limited to the 2016 election. It's a daily drumbeat. These [fake accounts] are entities trying to disrupt our democratic process by pushing various forms of disinformation into the system."[165] Influence campaigns, by the Russians and others,[166] have matured to the point where they are overwhelming social media's efforts to keep their platforms accountable. The polemics span the political spectrum with the goal of engendering online outrage and turning it into offline chaos.[167] Not all of these efforts rely on artificial intelligence; some are just good old psychological warfare. But AI enables today's information warriors to engage in even more sophistiaced activities.[168] Tailoring the latest propaganda to polarized Americans is precisely the type of game that psychographic profiling excels at.

We are wholly unprepared for this assault on democracy. Given the paucity of federal law regulating social media and privacy, little attention has been paid to the problem. Congress did hold hearings on the Cambridge Analytica data scandal two years after it occurred.[169] Mark Zuckerberg, the key witness, escaped unscathed with an apology for not "do[ing] enough to prevent these tools from being used for harm,"[170] and for not notifying the 87 million users whose data had been compromised. Although a spate of clever sounding bills

---

[165] Kevin Roose, *Facebook Grapples with a Maturing Adversary in Election Meddling*, N.Y. TIMES (Aug. 1, 2018), https://www.nytimes.com/2018/08/01/technology/facebook-trolls-midterm-elections.html.
[166] It appears that Iran has also begun significant influence operations aimed at shaping America's political discourse. *See* https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html.
[167] Digital Forensics Research Lab, *Troll Tracker: Facebook Uncovers Active Influence Operation*, MEDIUM (July 31, 2018), https://medium.com/dfrlab/trolltracker-facebook-uncovers-active-influence-operation-74bddfb8dc06.
[168] *Id.*
[169] *Facebook, Social Media Privacy, and the Use and Abuse of Data: Joint Hearing Before the S. Comm. on the Judiciary and on Commerce, Science and Transportation*, 115th Cong. (2018); *Facebook: Transparency and Use of Consumer Data: Hearing Before the H. Comm. on Energy and Commerce*, 115th Cong. (2018).
[170] *See Facebook, Social Media Privacy, and the Use and Abuse of Data: Joint Hearing Before the S. Comm. on the Judiciary and on Commerce, Science and Transportation*, 115th Cong. (2018) (written Testimony of Mark Zuckerberg at 1).

has been introduced,[171] no legislation has actually resulted from the hearings or elsewhere to respond to election hacking. Instead, Facebook has gone on a covert lobbying campaign to discredit its critics.[172] Zuckerberg has declined to appear before lawmakers in Britain and other countries to account for privacy lapses.[173]

Nor is self-regulation sufficient. Social media companies impose few restrictions on who can access user data. Rather, they actively share data with each other, usually without express opt-in consent.[174] A U.K. Parliamentary committee recently concluded that Facebook overrides its users privacy settings in order to maximize revenue.[175] Even when platforms try to police themselves, they wind up in a game of whac-a-mole. After they block one company, others may rise from the ashes. After being banned from Facebook amid a public outcry, Cambridge Analytica dissolved. But Facebook and other social media continue to profit from analytics companies using their vast repository of user data. For instance, the firm Crimson Hexagon claims to have lawfully collected more than 1 trillion posts and images from Facebook, Twitter, Instagram, Tumblr and other social media platforms.[176] Through the use of AI, Crimson can

---

[171] *See, e.g.*, Prevent Election Hacking Act of 2018, H.R. 6188; Securing America's Elections Act of 2018, HR. 5147; Helping State and Local Governments Prevent Cyber Attacks (HACK) Act, S. 1510 (2017).
[172] Sheera Frenkel et al., *Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis*, N.Y. TIMES (Nov. 14, 2018), https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html. Facebook's lapses have triggered a fine from the FTC as high as $5 billion. *See* Mike Isaac & Cecilia Kang, *Facebook Expects to Be Fined Up to $5 Billion by F.T.C. Over Privacy Issues*, N.Y. TIMES (Apr. 24, 2019), https://www.nytimes.com/2019/04/24/technology/facebook-ftc-fine-privacy.html.
[173] *See* Tony Romm, *Facebook Faces Fresh Lashing from Nine Countries for Its Inability To Stop the Spread of Fake News*, WASH. POST (Nov. 27, 2018), https://www.washingtonpost.com/technology/2018/11/27/facebook-faces-global-lashing-nine-countries-its-inability-protect-data-stop-fake-news.
[174] *See* Dance, *supra* note 51.
[175] Tony Romm, *Facebook 'Intentionally And Knowingly' Violated U.K. Privacy And Competition Rules, British Lawmakers Say*, WASH. POST (Feb. 17, 2019), https://www.washingtonpost.com/technology/2019/02/18/facebook-intentionally-knowingly-violated-uk-privacy-competition-rules-british-lawmakers-say.
[176] Olivia Solon & Julie Carrie Wong, *Facebook Suspends Another Analytics Firm Amid Questions Over Surveillance,* GUARDIAN (July 20, 2018), https://www.theguardian.com/technology/2018/jul/20/facebook-crimson-hexagon-analytics-data-surveillance.

perform sophisticated "sentiment analysis" for its clients.[177] Armed with knowledge of an individual's "sentiments" across a matrix of decision points, it is a short step for companies from persuasion to manipulation.

3. Fake News

Disinformation campaigns are old tools of war, diplomacy, negotiation and power politics. Fake news in ancient Rome may have sealed the fate of Mark Antony and Cleopatra.[178] AI adds more than effectiveness to info wars, it elevates them to a whole new dimension. As fake news competes with the real world in the popular discourse, and often crowds it out, people get inured to facts. Facts become denigrated as information sources for cognitive processing. Lacking facts for decision-making we turn to emotional cues such as authenticity, strength of assertion, feelings and beliefs. Donald Trump may be the most notable victim of this. His intelligence agency's factual findings of Russian interference in the 2016 election were no match for Vladimir Putin's "extremely strong and powerful" denial.[179] Like many humans, he simply prefers power to truth.

Fake news was another feature of the 2016 elections that has been weaponized by artificial intelligence. "Fake news" is a recently coined term that describes topical content that is fabricated, distorted, misleading or taken out of context. It is commonly distributed online and often "micro-targeted" to affect a particular group's opinions.[180] While false reporting, misdirection, and propaganda are

---

[177] *See* Garett Huddy, *What is Sentiment Analysis,* CRIMSON HEXAGON, https://www.crimsonhexagon.com/blog/what-is-sentiment-analysis (sentiment analysis (or "opinion mining") attempts to understand what people think or how they feel about a certain topic).

[178] *See* Eve Macdonald, *The Fake News That Sealed the Fate of Antony and Cleopatra,* THE CONVERSATION (Jan. 13, 2017), https://theconversation.com/the-fake-news-that-sealed-the-fate-of-antony-and-cleopatra-71287.

[179] Remarks by President Trump and President Putin of the Russian Federation in Joint Press Conference, July 16, 2018, https://www.whitehouse.gov/briefings-statements/remarks-president-trump-president-putin-russian-federation-joint-press-conference/

[180] *See generally* House of Commons, Digital, Culture, Media and Sport Committee, Disinformation and "fake news": Interim Report, July 29, 2018.

centuries old tactics, artificial intelligence compounds the problem of fake news by making it seem more realistic or relevant through targeted tailoring. "[F]ake news .. is particularly pernicious when disseminated as part of a complex political strategy that mines big data to hyper-target audiences susceptible to its message."[181] Unfortunately, purveyors of fake news are also able to exploit citizens' faith in autonomy and decisional privacy described in Part III.B. As historian Yuval Noah Harari notes, "The more people believe in free will… the easier it is to manipulate them, because they won't think that their feelings are being produced and manipulated by some external system."[182]

AI tools available on the internet actively promote rumor cascades and other "information disorders."[183] For instance, when the FCC was considering repealing Net Neutrality rules in 2017, 21 million of the 22 million comments the agency received were fakes or sent by bots and organized campaigns.[184] In the last three months of the 2016 election campaign, "top-performing false election stories from hoax sites and hyperpartisan blogs generated 8,711,000 shares, reactions, and comments on Facebook."[185] This was more than the number generated by the major news websites. Social media sites derive significant revenue from fake news, thus minimizing their incentive to police it.[186] Purveyors also make a good living by selling

---

[181] Lili Levi, *Real "Fake News" and Fake "Fake News,"* 16 FIRST AMEND. L. REV. 232, 253 (2017).
[182] Andrew Anthony, *Yuval Noah Harari: The Idea of Free Information is Extremely Dangerous*, GUARDIAN (Aug. 5, 2018), https://www.theguardian.com/culture/2018/aug/05/yuval-noah-harari-free-information-extremely-dangerous-interview-21-lessons.
[183] David M. J. Lazar et al., *The Science of Fake News*, 359 SCI. 1094, 1096 (2018).
[184] Mary Papenfuss, *Feds Investigating Millions of Fake Messages Opposing Net Neutrality: Report*, HUFFINGTON POST (Dec. 8, 2018, 9:14 PM), https://www.huffingtonpost.com/entry/feds-probe-fake-messages-to-fcc-supporting-ending-net-neutrality_us_5c0c4ae1e4b0ab8cf693ec5c.
[185] Craig Silverman, *This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook*, BUZZFEED (Nov. 16, 2016, 5:15 PM), https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook.
[186] *See* Peter Cohan, *Does Facebook Generate Over Half of Its Ad Revenue From Fake News?*, FORBES (Nov. 25, 2016), https://www.forbes.com/sites/petercohan/2016/11/25/does-facebook-generate-over-half-its-revenue-from-fake-

fake news on those sites; what is now called the "fake-view ecosystem."[187] Views can simply be bought as a way to increase rankings and enhance influence campaigns. At one point, "YouTube had as much traffic from bots masquerading as people as it did from real human visitors."[188] Similarly, Twitter retweets are much more likely to contain false information than true information.[189] False political news is more viral than any other category of false news.[190] Gartner predicts that by 2022, "the majority of individuals in mature economies will consume more false information than true information."[191] Brookings calls this "the democratization of disinformation."[192]

The business models of social media and news sites include reader comments. This too seems to be a democratizing feature of our online world. But, we've caught the tiger by the tail. Commenting, especially by internet trolls, "has opened the door to more aggressive bullying, harassment and the ability to spread misinformation."[193] As with other fake news, AI is used at both ends of this problem.[194] While tech companies employ "Captcha"[195] and other

---

news/#656383d8375f. Platforms even have immunity under the Communications Decency Act (CDA) for hosting false, damaging or infringing content. 47 U.S.C. § 230.

[187] Michael H. Keller, *The Flourishing Business of Fake YouTube Views*, N.Y. TIMES (Aug. 11, 2018), https://www.nytimes.com/interactive/2018/08/11/technology/youtube-fake-view-sellers.html.

[188] *Id*. *See also* Lazar, *supra* note 183, at 1094, 1095 (Facebook estimates that as many as 60 million social bots infest its platform).

[189] Lazar, *supra* note 183, at 1094-95.

[190] *Id*. at 1148; Soroush Vosoughi et al., *The Spread of True And False News Online*, 359 SCI. 1146 (2018).

[191] Kasey Panetta, *Gartner Top Strategic Predictions for 2018 and Beyond*, GARTNER (Oct. 3, 2017), https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions. For a survey of scientific studies on the flow of fake news, *see* Vosoughi et al., *supra* note 193.

[192] *Supra* note 141.

[193] Brian X. Chen, *The Internet Trolls Have Won. Sorry, There's Not Much You Can Do,* N.Y. TIMES (Aug. 8, 2018), https://www.nytimes.com/2018/08/08/technology/personaltech/internet-trolls-comments.html.

[194] *See* Tarek Ali Ahmad, *Artificial Intelligence a Tool for Those Creating and Combating Fake News*, ARAB NEWS (Apr. 4, 2018), http://www.arabnews.com/node/1278426/media.

[195] "Captcha" stands for "Completely Automated Procedures for Telling Computers and Humans Apart." Some procedures are as simple as asking a poster to check a box confirming that she is not a robot.

methods to detect bots and spammers,[196] including third-party services,[197] hackers use more sophisticated means to hijack websites[198] or simply float their own apps on Apple and Google app stores.[199] Ultimately, "when it comes to fake news, AI isn't up to the job.".[200]

Facebook and Google have a "complicated relationship" with AI and fake news.[201] On the one hand, they employ AI to filter fake news[202] and remove fake accounts and users engaged in political influence campaigns.[203] At the same time, they seem to profit nicely from fake news and have been strongly criticized for deliberately inadequate policing.[204] For example, Google's YouTube also profits nicely from fake news. Its "recommendation algorithm" serves "up next" video thumbnails that its AI program determines will be of interest to each of its 1.5 billion users. The algorithm, which "is the single most important engine of YouTube's growth," revels at promoting conspiracy theories.[205] While most of the attention has been directed at Facebook and Twitter, "YouTube is the most overlooked

---

[196] *See, e.g.,* http://fakenewschallenge.org
[197] *See* Jackie Snow, *Can AI Win the War Against Fake News?*, MIT TECH. REV. (Dec. 13, 2017), https://www.technologyreview.com/s/609717/can-ai-win-the-war-against-fake-news.
[198] Chen, *supra* note 193.
[199] Jack Nicas, *Tech Companies Banned Infowars. Now, Its App Is Trending*, N.Y. TIMES (Aug. 8, 2018), https://www.nytimes.com/2018/08/08/technology/infowars-app-trending.html.
[200] James Vincent, *Why AI Isn't Going to Solve Facebook's Fake News Problem*, VERGE (Apr. 5, 2018), https://www.theverge.com/2018/4/5/17202886/facebook-fake-news-moderation-ai-challenges.
[201] Jonathan Vanian, *Facebook's Relationship with Artificial Intelligence and Fake News: It's Complicated*, FORTUNE (Dec. 1, 2016), http://fortune.com/2016/12/01/facebook-artificial-intelligence-news.
[202] *See, e.g.*, James Vincent, *Facebook Is Using Machine Learning To Spot Hoax Articles Shared By Spammers*, THE VERGE (June 21, 2018), https://www.theverge.com/2018/6/21/17488040/facebook-machine-learning-spot-hoax-articles-spammers.
[203] Nicholas Fandos & Kevin Roose, *Facebook Identifies an Active Political Influence Campaign Using Fake Accounts*, N.Y. TIMES (July 31, 2018), https://www.nytimes.com/2018/07/31/us/politics/facebook-political-campaign-midterms.html.
[204] *See supra* note 173.
[205] Lewis, *supra* note 158.

story of 2016.… Its search and recommender algorithms are misinformation engines."[206] One exposé has found that "YouTube systematically amplifies videos that are divisive, sensational and conspiratorial."[207]

A particularly effective instance of fake news is called "deepfakes," which is audio or video that has been fabricated or altered to deceive our senses.[208] While "Photoshop" has long been a verb as well as a graphics program, AI takes the deception to a whole new level. Consider the program FakeApp, which allows users to alter faces into videos.[209] It is popularly used for celebrity face-swapping pornography and having politicians appear to say humorous or outrageous things.[210] Generative adversarial networks (GANs) take this one step further, by playing one network against another in generating or spotting fake images. In such cases, "[t]he AI trying to detect fakery always loses."[211]

Problems of fake news will get much worse as these tools become commonplace. Large-scale unsupervised algorithms can now produce synthetic text of unprecedented quality,[212] which have the potential to further blur the line between reality and fakery. With that in mind, the developer of one such product has declined to publically

---

[206] *Id. See also* Zeynep Tufekci, *Algorithmic Harms Beyond Facebook and Google: Emergent Challenges Of Computational Agenc*y, 13 COLO. TECH. L.J. 203, 216 (2015).
[207] *Id.* (citing findings available at algotransparency.org).
[208] See generally Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. (forthcoming 2019).
[209] *See* Adi Robertson, *I'm using AI to face-swap Elon Musk and Jeff Bezos, and I'm really bad at it,* VERGE (Feb. 11, 2018 12:00 PM), https://www.theverge.com/2018/2/11/16992986/fakeapp-deepfakes-ai-face-swapping.
[210] To see this in action, visit https://www.thispersondoesnotexist.com, which uses AI to generate completely fictitious but realistic fake faces.
[211] Cade Metz, *How Will We Outsmart A.I. Liars*?, N.Y. TIMES (Nov. 19, 2018), https://www.nytimes.com/2018/11/19/science/artificial-intelligence-deepfakes-fake-news.html.
[212] *See* OpenAI, *Better Language Models and Their Implications*, https://blog.openai.com/better-language-models.

release the code "[d]ue to our concerns about malicious applications of the technology."[213]

The risks are not overstated. As one article warned, "imagine a future where … a fake video of a president incites a riot or fells the market."[214] Or as *The Atlantic*'s Franklin Foer puts it, "We'll shortly live in a world where our eyes routinely deceive us. Put differently, we're not so far from the collapse of reality."[215] Brian Resnick of *Vox* is even more pessimistic. "[I]t's not just our present and future reality that could collapse; it's also our past. Fake media could manipulate what we remember, effectively altering the past by seeding the population with false memories."[216] Humans are susceptible to such distortions of reality.[217] An old Russian proverb may soon come true: "the most difficult thing to predict is not the future, but the past."[218]

"The collapse of reality isn't an unintended consequence of artificial intelligence. It's long been an objective – or at least a dalliance – of some of technology's most storied architects" argues Franklin Foer.[219] Unplugging reality is also the domain of Virtual Reality (VR) and Augmented Reality (AR) technologies. We've come to appreciate these as enhancing gaming experiences and entertainment. Will we also appreciate them as they distort democracy and individual rights?

---

[213] *Id.*
[214] Brian Resnick, *We're Underestimating the Mind-Warping Potential of Fake Video*, VOX (July 23, 2018), https://www.vox.com/science-and-health/2018/4/20/17109764/deepfake-ai-false-memory-psychology-mandela-effect. *See also* Kenneth Rapoza, *Can "Fake News" Impact The Stock Market?*, FORBES (Feb. 26, 2017), https://www.forbes.com/sites/kenrapoza/2017/02/26/can-fake-news-impact-the-stock-market/#40d121c2fac0 (discussing a $130 billion drop in stock value after a tweet in 2013 falsely claiming that President Obama had been injured in an explosion).
[215] Franklin Foer, *The Era of Fake Video Begins*, ATLANTIC (May 2018), https://www.theatlantic.com/magazine/archive/2018/05/realitys-end/556877.
[216] Resnick, *supra* note 214.
[217] *Id*. (citing Elizabeth Loftus, U. Cal. Irvine).
[218] Lawrence Rosen, The Culture of Islam: Changing Aspects of Contemporary Muslim Life 98.
[219] Foer, *supra* note 215.

However, AI could also help provide potential solutions to the challenge of fake news. Fact checking organizations such as Politifact go after the most potent falsehoods, but so much fake news abounds that fact checking has become its own industry with its own set of standards and principles.[220] Algorithms could also help mitigate the problem. Google has funded Full Fact to develop an AI fact-checking tool for journalists.[221] Other such services are cropping up.[222] Page ranking can also be tweaked to discount identified misinformation. However, fact checking can be counterproductive since repeating false information, even in the context of correction, can "increase an individual's likelihood of accepting it as true."[223] Thus, at the end of the day, the advantage goes to fake news. Its purveyors can rely on AI, the First Amendment, social media companies' profit motive, and the political payoff of successful fake news campaigns. For Milton it was sufficient to "let [Truth] and Falsehood grapple; who ever knew Truth put to the worse, in a free and open encounter?"[224] Of course, that was long before AI altered the playing field.

4. Demise of Trusted Institutions

Fake news not only manipulates elections, it also obstructs the levers of democracy, the most important of which is a free press. The institutional press had, over the 20th century, developed journalistic norms of objectivity and balance. But the rise of digital publishing allowed many new entrants – both challenging traditional norms and cutting into the profits of the institutional press.[225]

The abundance of fake news is accompanied by claims that unfavorable but factual news is itself fake. By sowing seeds of distrust, false claims of fake news are designed to erode trust in the press, "which

---

[220] *See* UK Disinformation Report, at 8, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.
[221] *See* Matt Burgess, *Google is helping Full Fact create an automated, real-time fact-checker,* WIRED UK (Nov. 17, 2016), https://www.wired.co.uk/article/automated-fact-checking-full-fact-google-funding.
[222] *See* UK Disinformation Report, fn. 25.
[223] Lazar, *supra* note 183, at 1095.
[224] JOHN MILTON, AREOPAGITICA 58 (Cambridge U. Press 1644).
[225] Lazar, *supra* note 183.

collapsed to historic lows in 2016."[226] Anti-press rhetoric, such as that journalists are "the enemy of the people," further erodes democratic ideals.[227] As mainstream media withers under these attacks, social media feeds take its place, enhanced by algorithmic targeting as described above.[228] Some claim these non-traditional means democratize the production and delivery of news. They surely do increase the number of voices that get heard, especially of unpopular and anti-establishment views. However, much gets lost in the cacophony of noise. Moreover, the self-selection that social media channels enable means that many people are never exposed to contrary views. Their news consumption resembles an echo chamber. Pre-existing biases are simply reinforced. When it comes to fact finding, AI is a "competency destroying technology."[229]

Most Americans get their news from social media, which has assumed the roles of news source, town square and speaker's corner. Internet giants determine, without regard to the First Amendment, who gets to be seen and heard. News-filtering algorithms serve a gate-keeping function on our consumption of content. Moderators may try to be even handed and open minded, but they also face market forces that tend to reduce content to the least common denominator.[230] Viewer counts, page views and clicks are the established metrics of success. "Big data and algorithms have shaped journal-

---

[226] *Id.* (only 51% of Democrats and 14% of Republicans expressed trust in mass media as a news source).

[227] *Statement of A.G. Sulzberger, Publisher, The N.Y. Times, In Response to President Trump's Tweet About Their Meeting*, N.Y. TIMES (July 29, 2018), https://www.nytco.com/press/statement-of-a-g-sulzberger-publisher-the-new-york-times-in-response-to-president-trumps-tweet-about-their-meeting (noting that President Trump's attacks on the press could lead to violence against reporters).

[228] *See* Economist Intelligence Unit, *Democracy Index 2017*, at 44, https://pages.eiu.com/rs/753-RIQ-438/images/Democracy_Index_2017.pdf (social media has "presented a major challenge to the economic viability of news publishers and broadcasters").

[229] The phrase, although not necessarily the context, is attributable to Cornelia Dean, former Science Editor, The New York Times.

[230] Of course, moderators are seldom neutral. "A manager of public Facebook page selects to disseminate specific posts at his discretion … and can personalize the dissemination … using complex algorithms and artificial intelligence." Michal Lavi, *Taking Out of Context*, 31 HARV. J.L. & TECH, 145, 153-54 (2017).

istic production, ushering in an era of `computational journalism'."[231] The marketplace of ideas is relegated to secondary status. Robots are even writing news stories for major outlets.[232] Once the fourth estate is debilitated, "democracy dies in darkness."[233]

B. Equality and Fairness

Essential to theories of liberal democracy are principles of due process, equality, and economic freedom. These values too are embedded in foundational and human rights documents. Consider the Declaration of Independence proclamation that "all men are created equal" with "unalienable Rights… [to] Life, Liberty and the pursuit of Happiness.—That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed."[234] No clearer expression has emerged of the link between equality, due process and democracy.

Due process and equal protection comprise "a coherent scheme of equal basic liberties with two themes: securing the preconditions for deliberative autonomy as well as those of deliberative democracy."[235] Judicial intervention under the due process and equal protection clauses is most appropriate when governmental action distorts the political process.[236] And, of course, Justice Stone's famous footnote four in *United States v. Carolene Products* makes a principled connection between equality and the political process.[237]

The realization of equality under law has become more difficult in the digital age. This is partially due to Supreme Court doctrines such as the "state action doctrine" and the "requirement of purpose." The

---

[231] Samantha Shorey & Philip N. Howard, *Automation, Big Data, and Politics*, 10 INT'L J. OF COM'N 5037 (2016).
[232] *See* Lucia Moses, *The Washington Post's Robot Reporter Has Published 850 Articles In The Past Year*, DIGIDAY (Sept. 14, 2017), https://digiday.com/media/washington-posts-robot-reporter-published-500-articles-last-year.
[233] Slogan of the Washington Post.
[234] The Declaration of independence para. 2 (U.S. 1776).
[235] James E. Fleming, *Constructing the Substantive Constitution*, 72 TEX. L. REV. 211, 274 (1993).
[236] *See* JOHN HART ELY, DEMOCRACY AND DISTRUST (1980).
[237] 304 U.S. 144, 152, n.4 ("prejudice against discrete and insular minorities … tends seriously to curtail the operation of those political processes ordinarily to be relied upon to protect minorities").

former exempts private actors from constitutional constraint.[238] Many of our most vital social structures are now in private hands, and thus not bound by the Fourteenth Amendment. For instance, the world governing body of the internet, the Internet Corporation for Assigned Names and Numbers (ICANN), is a private California corporation, and does not need to observe constitutional due process or speech rights.[239] Telecommunications and platform giants have First Amendment rights, but not corresponding obligations to ensure free speech for their users. Their functionally complete control of the means of communication in the digital age results in a vast transfer of rights from citizens to corporate directors, who owe fidelity to shareholders, not to the constitution.

The second doctrine mentioned, the "requirement of purpose," reads an intentionality requirement into the Equal Protection clause.[240] An action causing discriminatory results is not unconstitutional unless the discrimination was intended. Intent usually requires a human actor. Thus, decisions made or influenced by algorithm may be beyond constitutional reach no matter how biased or opaque they are.[241]

1. Opacity: Unexplained AI

One major downside to machine learning techniques is their opacity. Because the algorithms are not directly created by humans, the actual reasoning process used by them may be unknown and unknowable. Even if one could query the machine and ask what algorithms and factors it used to reach a particular outcome, the machine may not know. That is because neural networks many layers deep with millions of permutations are in play at any given time, adjusting their connections randomly or heuristically on a millisecond

---

[238] *See generally* Erwin Chemerinsky, *Rethinking State Action*, 80 NW U.L. REV. 503 (1985).
[239] *See* A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L. J. 17, 94-105, 141-42 (2000). But see Kate Klonick, *The New Governors: The People, Rules, And Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1602 (2018) (arguing that social media platforms respect the First Amendment "by reflecting the democratic culture and norms of their users").
[240] Washington v. Davis, 426 U.S. 229 (1976).
[241] Yavar Bathaee, *The Artificial Intelligence Black Box And The Failure Of Intent And Causation*, 31 HARV. J.L. & TECH. 889, 891 (2018).

scale.[242] It is like asking a turtle why its species decided to grow a shell. We know it was adaptive, but may not know the precise pathway taken to reach its current state. Our ignorance may actually be worse than that since we also cannot know if the AI is lying to us regarding its reasoning process. If one of the goals programmed into AI is to maximize human well-being that might be achieved by deceiving its human handlers now and then.[243]

Google's Ali Rahimi recently likened AI technology to medieval alchemy. Researchers "often can't explain the inner workings of their mathematical models: they lack rigorous theoretical understandings of their tools… [Yet], we are building systems that govern healthcare and mediate our civic dialogue [and] influence elections."[244] These problems are not mere conjecture or alarmist. One of the best-funded AI initiatives by the Department of Defense (DoD) is its Explainable AI (XAI) project. The DoD is concerned that drones and other autonomous devices may make questionable "kill" decisions, and there would be no way for humans in the chain of command to know why.[245]

[T]he effectiveness of [autonomous] systems is limited by the machine's current inability to explain their decisions and actions to human users … Explainable AI—especially explainable machine

---

[242] *See* Shaw, *supra* note 5.
[243] *See* George Dvorsky, *Why We'll Eventually Want Our Robots to Deceive Us*, GIZMODO (Oct. 4, 2017), https://gizmodo.com/why-well-eventually-want-our-robots-to-deceive-us-1819114004. Robots might even lie to each other if that produced some advantage; Bill Christensen, *Robots Learn to Lie*, LIVE SCIENCE (Aug. 24, 2009), https://www.livescience.com/10574-robots-learn-lie.html.
[244] John Naughton, *Magical Thinking About Machine Learning Won't Bring The Reality of AI Any Closer*, GUARDIAN (Aug. 5, 2018), https://www.theguardian.com/commentisfree/2018/aug/05/magical-thinking-about-machine-learning-will-not-bring-artificial-intelligence-any-closer. See also Steven Strogatz, *One Giant Step for a Chess-Playing Machine*, N.Y. TIMES (Dec. 26, 2018), https://www.nytimes.com/2018/12/26/science/chess-artificial-intelligence.html ("What is frustrating about machine learning, however, is that the algorithms can't articulate what they're thinking. We don't know why they work, so we don't know if they can be trusted.").
[245] *See* David Gunning, *Explainable Artificial Intelligence (XAI),* https://www.darpa.mil/program/explainable-artificial-intelligence.

learning—will be essential if future warfighters are to understand, appropriately trust, and effectively manage an emerging generation of artificially intelligent machine partners.[246]

Opaque AI outcomes are hidden by "black box" algorithms. Since we often do not know how an AI machine reached a particular conclusion, we cannot test that conclusion for compliance with legal and social norms, whether the laws of war or constitutional rights. If a machine returns a discriminatory result, say in sentencing or insurance risk rating, what would it mean to ask if that result were "intended"? How would we know if the result were arbitrary or capricious in a due process sense? As legal precepts, intentionality and due process are mostly incompatible with AI. The problem magnifies as we give AI more tasks and hence more power, which may ultimately lead to "law[making] by robot."[247] Notwithstanding the risks, we are already asked to trust AI-adjudicated decisions at federal agencies[248] and AI-generated evidence in court.[249] For some, the ultimate goal of AI development is "to get rid of human intuition."[250]

A further challenge is that judges and government agencies do not write the AI programs they use. Rather, they license them from private vendors. This act of licensing already trained AI or related

---

[246] *Id*.

[247] Gary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 GEO. L.J. 1147, 1147 (2017) (conducting an examination of whether current and future use of robotic decision tools such as risk assessment algorithms (law by robot) can hold muster under administrative or constitutional law).

[248] *Id.* Stanford Law School has a new practicum entitled "Administering by Algorithm: Artificial Intelligence in the Regulatory State." https://law.stanford.edu/education/only-at-sls/law-policy-lab/practicums-2018-2019/administering-by-algorithm-artificial-intelligence-in-the-regulatory-state.

[249] Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 2021-22 (2017). Similar problems arise with "forensic robots" who are increasingly being used to gather evidence in sensitive situations, such as child abuse cases. A robot may be superior to a human in that context, but can it proffer expert testimony? *See* Zachary Henkel & Cindy L. Bethel, *A Robot Forensic Interviewer*, J. HUMAN-ROBOT INTERACTIONS (2017).

[250] John Bohannon, *The Cyberscientist*, 357 SCI. 18, 18-19 (2018).

"transferred learning" techniques heightens opacity issues. Agencies not only lack transparency into the functionality and conclusions of the products they use, but also lack ownership of and access to examine the underlying data. The Supreme Court has made it difficult to patent software, so developers typically resort to trade secrets to preserve value in their AI investments.[251] Thus, firms are reluctant to disclose details even in the face of constitutional challenge.[252] Yet, there are no federal legal standards or requirements for inspecting the algorithms or their "black box" decisions. The Defend Trade Secrets Act of 2016[253] gives developers further ammunition to resist disclosure of their source code.[254]

The resulting lack of transparency has real world consequences. In *State v. Loomis*, defendant Eric Loomis was found guilty for his conduct in a drive-by shooting.[255] Loomis' answers to a series of questions were entered into COMPAS, a risk-assessment tool created by a for-profit company, Northpointe,[256] which returned a "high risk" recidivism score for him.[257] Loomis appealed, specifically challenging his sentence because he was not given the opportunity to assess the algorithm.[258] The Wisconsin Supreme Court rejected Loomis's challenge, reasoning that, according to a *Wired* report, "knowledge of the algorithm's output was a sufficient level of transparency."[259] The court also held that the human judge in the case could accept or

---

[251] *See* Alice Corp. v. CLS Bank Int'l, 573 U.S. 208 (2014).
[252] *See, e.g.*, People v. Billy Ray Johnson, No. F071640 (Cal. App. pending, 2018) (challenging for lack of access to a proprietary DNA-matching algorithm, TrueAllele, that evaluates the likelihood that a suspect's DNA is present at a crime scene).
[253] 18 U.S.C. § 1836, et seq.
[254] *See, e.g.,* Video Gaming Techs, Inc. v. Castle Hill Studios LLC, 2018 U.S. Dis. Lexis 118919 (using DTSA to protect proprietary algorithm where state trade secret law was inadequate).
[255] State v. Loomis, 881 N.W.2d 749 (Wis. 2016).
[256] *See COMPAS Risk & Need Assessment System: Selected Questions Posed by Inquiring Agencies*, NORTHPOINTE (2012), http://www.northpointe-inc.com/files/downloads/FAQ_Document.pdf.
[257] *See Loomis*, 881 N.W.2d 749 at 755.
[258] *See id.* at 753.
[259] Jason Tashea, *Courts Are Using AI to Sentence Criminals. That Must Stop Now*, WIRED (April 17, 2017, 7:00 AM), https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now.

reject the Compas score, so the AI algorithm was not actually determining the sentence, just suggesting it.[260]

We can expect further resort to legal formalism as the deployment of AI expands. A growing number of states use COMPAS or similar algorithms to inform decisions about bail, sentencing, and parole.[261] Further, even well intentioned bail and sentencing reforms can have pernicious effects when AI is involved.[262]

Some proponents justify the use of AI as a means to produce more consistent results and conserve resources in the criminal justice system.[263] That it does. But it also produces demonstrably discriminatory results. A study conducted by Pro Publica found that AI-generated recidivism scores in Florida "proved remarkably unreliable in forecasting violent crime" and were only "somewhat more accurate than a coin flip."[264] The algorithm was "particularly likely to falsely flag black defendants as future criminals, wrongly labeling them this way at almost twice the rate as white defendants."[265] Not only does this violate equality precepts, the inability of either judges or defendants to look into the "black box" of recommended outcomes threatens due process.[266]

---

[260] *See Loomis*, 881 N.W.2d 749 at 753. The lower court noted that Wisconsin judges routinely rely on COMPAS in sentencing, and did so in Loomis' case. *State v. Loomis*, 2015 Wisc. App. LEXIS 722, *2 (2015).
[261] EPIC, *Algorithms in the Criminal Justice System,* https://epic.org/algorithmic-transparency/crim-justice.
[262] *See* Sam Levin, *Imprisoned by Algorithms: The Dark Side of California Ending Cash Bail*, GUARDIAN (Sept. 7, 2018), https://www.theguardian.com/us-news/2018/sep/07/imprisoned-by-algorithms-the-dark-side-of-california-ending-cash-bail (discussing a California law which replaced cash bail with "risk assessment" tools but was feared to enable an increase in pre-trial incarceration).
[263] *Id*.
[264] Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016).
[265] *Id*.
[266] Tashea, *supra* note 259.

2. Algorithmic Bias

Objectivity is not one of AI's virtues. Rather, algorithms reflect back the biases in the programming that are input when models are designed and in the data used to train them. Additionally, while data analysis can identify relationships between behaviors and other variables, relationships are not always indicative of causality. Therefore, some data analysis can develop imperfect information caused by algorithmic limitations or biased sampling. As a result, decisions made by AI may intensify rather than remove human biases contrary to popular conception. [267] This poses real risks for equality and democracy.

The main problem with "algorithmic bias" is the data that is used to "train" the AI how to solve problems. In the law context, typically, factors from the real world, such as those reported in a judicial opinion, are fed into the computer, along with doctrinal rules describing how the law is applied to the facts. The AI is likely to return a wrong answer (measured against the result in the training case) on the first try, and maybe on the hundredth try. But because of machine learning, the AI adapts its algorithms until it eventually finds ones that return the same result as that of the training cases all or most of the time. However, training data can itself be biased, a feature that is simply amplified once the AI is let loose on a new set of facts. So, for instance, if historical data in criminal sentencing or crime statistics is racially biased, then the AI will be too each time it is used to recommend a sentence. The risks of training AI with inaccurate or biased data are also clear from the example of Microsoft's Tay, a "teen-talking AI chatbot built to mimic and converse with users in real time."[268] Due to Tay's machine learning capabilities, she was making racist and discriminatory tweets within a few hours.[269] She was not designed to be human proof and block malicious intent. As

---

[267] Justin Sherman, *AI And Machine Learning Bias Has Dangerous Implications*, OPEN-SOURCE (Jan. 11, 2018), https://opensource.com/article/18/1/how-open-source-can-fight-algorithmic-bias (saying that "data itself might have a skewed distribution").
[268] Sophie Kleeman, *Here Are the Microsoft Twitter Bot's Craziest Racist Rants*, GIZMODO (Mar. 24, 2016), https://gizmodo.com/here-are-the-microsoft-twitter-bot-s-craziest-racist-ra-1766820160.
[269] *Id*.

Tay shows, AI functions can mirror and amplify societal biases and infirmities, only with the veneer of impartiality.[270]

Not only is training data often biased, but so too are the larger data sets subsequently used to produce AI outcomes. Input data is generated either by humans or sensors that are designed by humans. Data selection, interpretation and methodologies are also of human design and may reflect human biases. Thus, "flaws—ethical or methodological—in the collection and use of big data may reproduce social inequality."[271] Algorithms make subjective decisions, including "classification, prioritization, association, and filtering . . . . They transform information, and they have social consequences."[272]

Automated classification is known to produce discriminatory outcomes. One example is AI classification of images, which occurs in facial recognition software. Often it does not detect dark skin, or even classifies black subjects as gorillas.[273] Another example is Google's search algorithm, which returns results reflecting occupational gender stereotypes.[274] Its autocomplete algorithm can also elicit suggestions associated with negative racial stereotypes.[275] Similar results occur when training data oversamples white males and undersamples women and minorities in positions of power or

---

[270] *See* Glen Meyerowitz, *There Is Nothing Either Good or Bad, But Training Sets Make It So*, 2 J. ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW 17, 20-22 (2019). Training data can also be "contaminat[ed]" by cyberattackers introducing false data in a technique known as "adversarial machine learning." *See The National Artificial Intelligence Research and Development Strategic Plan*, NAT'L SCI. & TECH. COUNCIL 30 (Oct. 2016), https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf.

[271] Shorey & Howard, *supra* note 231.

[272] *Id*.

[273] *See* Conor Dougherty, *Google Photos Mistakenly Labels Black People 'Gorillas'*, N.Y. TIMES (July 1, 2015, 7:01PM), https://bits.blogs.nytimes.com/2015/07/01/google-photos-mistakenly-labels-black-people-gorillas.

[274] Matthew Kay, Cynthia Matuszek & Sean A. Munson, *Unequal Representation and Gender Stereotypes in Image Search Results for Occupations*, in Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (2015), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.697.9973&rep=rep1&type=pdf.

[275] Issie Lapowsky, *Google Autocomplete Still Makes Vile Suggestions,* WIRED (Feb. 12, 2018, 11:09 AM), https://www.wired.com/story/google-autocomplete-vile-suggestions.

prestige.[276] This allows Amazon to create a "database of suspicious persons" for its home automation technologies.[277]

It is impossible to strip bias from human beings, but it may be possible to remove bias from AI with the proper governance of data input. Do we want AI to reflect the stereotypes and discrimination prevalent in society today, or do we want AI to reflect a better society where all people are treated as equal? Timnit Gebru, co-founder of the Black in AI event, advocates that diversity is urgently needed in AI.[278] This means more than a variety of people working on technical solutions and includes diversity in data sets and in conversations about law and ethics. If data sets are not diverse, then data output is going to be biased. Governance over data input is thus necessary to ensure it is vast, varied, and accurate.

IV. REGULATION IN THE AGE OF AI

Currently, there are no regulations in the United States specific to artificial intelligence.[279] Instead, applications of AI are regulated, if at all, under a hodgepodge of "privacy, cybersecurity, unfair and deceptive trade acts and practices, due process, and health and safety" laws.[280] Two things are missing from that regulatory landscape.

---

[276] *See* Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399, 411-12 (2017).

[277] Peter Holley, *This Patent Shows Amazon May Seek To Create A "Database Of Suspicious Persons" Using Facial-Recognition Technology*, WASH. POST (Dec. 18, 2018), https://www.washingtonpost.com/technology/2018/12/13/this-patent-shows-amazon-may-seek-create-database-suspicious-persons-using-facial-recognition-technology.

[278] Jackie Snow, *"We're in a Diversity Crisis": Cofounder of Black in AI on What's Poisoning Algorithms in Our Lives*, MIT TECH. REV. (Feb 14, 2018), https://www.technologyreview.com/s/610192/were-in-a-diversity-crisis-black-in-ais-founder-on-whats-poisoning-the-algorithms-in-our.

[279] In December 2017, the Fundamentally Understanding the Usability and Realistic Evolution (FUTURE) of Artificial Intelligence Act of 2017 was introduced, but has not yet passed. It would be the first U.S. legislation to "focus on forming a comprehensive plan to promote, govern, and regulate AI." John Weaver, *United States: Everything is Not Terminator: America's First AI Legislation,* (Aug. 3, 2018), MONDAQ, http://www.mondaq.com/united-states/x/724056/new+technology/The+content+of+this+article+is+intended+to+provide+a+general+guide; *see also infra* note 393.

[280] Christopher Fonzobe & Kate Heinzelman, *Should the Government Regulate Artificial Intelligence? It Already Is*, THE HILL (Feb. 26, 2018, 12:00 PM),

First is adequate protection of privacy interests and democratic values. Second is an appreciation of the unique challenges that AI presents. It has been over thirty years since Congress passed the last substantial privacy law.[281] If it takes that long to tackle the challenges of AI, the world is likely to be a very different place by the time Congress gets around to acting. This section examines the current regulatory framework in the United States and how it differs from European law. It concludes with proposals to modernize regulations to meet the challenges of AI.

A. Patchwork of Privacy Protections in the United States

The United States is home to some of the largest and most advanced technology and data companies in the world. Scholars attribute their dominance in the international marketplace to the lack of a comprehensive federal regulation protecting personal data and informational privacy. Instead, the United States relies on a "sectoral approach," which consists of a smorgasbord of industry-specific federal laws, often enforced by different agencies and providing diverse standards.[282] These are supplemented by state privacy laws, self-regulatory guidelines, and general-purpose consumer protection laws.[283]

In contrast, the European Union (EU) and many other developed countries follow an omnibus approach with one law regulating data collection, use, and sharing consistently across industries. For example, the EU's General Data Protection Regulation (GDPR)[284] is a broad regulation that applies across sectors and member states to all entities "established" within the EU, offering goods or services

---

http://thehill.com/opinion/technology/375606-should-the-government-regulate-artificial-intelligence-it-already-is.

[281] *See* Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22.

[282] Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACH PRIVACY (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law.

[283] *See id.*

[284] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

in the EU, or monitoring people in the EU.[285] The latter features make extra-territorial application and enforcement against U.S. companies a real possibility.

Many U.S. businesses initially preferred the sectoral approach as to tailor regulations to their nuanced needs. While there is some validity to that model, it also facilitates regulatory capture, industry lobbying, and privacy abuses often falling through regulatory cracks. The sectoral approach has created a patchwork system of state and federal laws that "overlap, dovetail and contradict one another."[286]

Among the most important federal laws are: HIPAA (personally identifiable health information), [287] GLBA (financial information),[288] the Telephone Consumer Protection Act (TCPA) (telemarketing),[289] the CAN-SPAM Act (spam email),[290] the Computer Fraud and Abuse Act (CFAA) (hacking),[291] and ECPA (electronic communications).[292] Each law is also enforced by a different agency or state body. It is hard to develop a coherent privacy policy with such a scattershot regime.

Recently, states in reaction to Cambridge Analytica have begun enacting their own privacy regulations to give their residents enhanced privacy protections and supplement gaps in federal laws.[293] This further complicates the patchwork system of federal and existing state regulations technology companies must comply with. As a result, for the first time, technology companies have started lobbying

---

[285] *Id*. art. III.
[286] Ieuan Jolly, *Data Protection in the United States: Overview*, THOMAS REUTERS PRACTICAL LAW (July 1, 2017), https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html.
[287] 42 U.S.C. §1301 et seq.
[288] 15 U.S.C. §§6801-6827.
[289] 47 U.S.C. §227 et seq.
[290] 15 U.S.C. §§7701-7713 and 18 U.S.C. §1037.
[291] 18 U.S.C. §1030.
[292] 18 U.S.C. §2510.
[293] *See* Neema Singh Guliani, *The Tech Industry is Suddenly Pushing for Federal Privacy Legislation. Watch Out.,* WASH. POST (Oct. 3, 2018), https://www.washingtonpost.com/opinions/the-tech-industry-is-suddenly-pushing-for-federal-privacy-legislation-watch-out/2018/10/03/19bc473e-c685-11e8-9158-09630a6d8725_story.html.

for federal legislation to preempt state laws like California's Consumer Privacy Act (CCPA).

1. State Privacy Laws

State laws often fill holes left by federal statutes, but this adds to the patchwork of privacy law, particularly with data-breach notification statutes. All states require that individuals be notified when their information has been compromised, usually through cyberattack, but state laws often have dissimilar and incompatible requirements.[294] For example, "New Jersey requires that the state police cybercrime unit be notified of breach, while Maryland requires that the state attorney general be notified before any affected individual is."[295] Illinois considers biometric data to be "personal information" triggering breach notification unlike many other states.[296] California's "wall of shame" catalogs all cyber breaches affecting residents.[297] This indicates just how severe the problem is, not just for individuals, but also for businesses that have to comply with the smorgasbord of state and federal laws. Privacy compliance may be a new full-time employment opportunity for lawyers.

California's Online Privacy Protection Act of 2003 (CalOPPA) requires operators of online services that collect "personally identifiable information" (PII) to post privacy policies that include: what

---

[294] *See Security Breach Notification Laws,* NAT'L CONF. ST. LEGIS. (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[295] Dana B. Rosenfeld et al. *State Data Breach Laws Agency Notice Requiremewnts Chart: Overview*, THOMSON REUTERS (2019), https://1.next.westlaw.com/Document/I1559f980eef211e28578f7ccc38dcbee/View/FullText.html.
[296] Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14/10 (2008).
[297] *See* Xavier Becerra, Attorney General, *Search Data Security Breaches*, STATE OF CA. DEPT. OF JUSTICE, https://www.oag.ca.gov/privacy/databreach/list (last visited Aug. 1, 2018).

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.[298]

Due to California's economic importance and the borderless world of ecommerce, the impact of this legislation transcends state borders and forces all technology companies to comply. The problem is that no one reads or understands the technical legalese privacy policies and terms of service agreements contain. According to Carnegie Melon researchers, it would take 76 days at 8 hours per day to read all the privacy policies one typically encounters.[299]

CalOPPA is supplemented by the newly enacted California Consumer Privacy Act (CCPA).[300] This is the most expansive privacy regime in the country and resembles Europe's omnibus approach.[301] It protects types of data that were previously not protected under U.S. privacy laws such as purchasing history, browsing and search history, and inferences drawn from PII.[302] CCPA creates four individual rights giving California residents more control over their data, including the rights to delete, receive information and copies of their data, opt-out and be free from discrimination. Enforcement of the CCPA may take place through enforcement actions by the California Attorney General or limited private rights of action.[303]

---

[298] *See* Kamala D. Harris, *Making Your Privacy Practices Public*, STATE OF CA. DEPT. OF JUSTICE 1 (May 2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf.

[299] Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, ATLANTIC (Mar. 1, 2012), https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days.

[300] CAL. CIV. CODE §§ 1798.100–1798.198 (2018).

[301] Many states are considering copying California's CCPA. *See* Davis Wright, *"Copycat CCPA" Bills Introduced in States Across Country*, JD SUPRA (Feb. 8, 2019), https://www.jdsupra.com/legalnews/copycat-ccpa-bills-introduced-in-states-20533.

[302] CAL. CIV. CODE § 1798.140(o)(1). Personal information is broadly defined to capture any information that is "capable of being associated with" a California resident, household or device. *Id.* The definition is arguably broader than "personal data" under GDPR.

[303] CAL. CIV. CODE §1798.160.

Recently, California has turned up the heat on privacy and cybersecurity legislation by passing laws regulating IoT and chatbots. Effective January 1, 2020, manufacturers of any IoT or smart device must implement reasonable security features preventing unauthorized access, information disclosure,[304] or modification.[305] Moreover, effective July 1, 2019, chatbots must identify themselves and cannot pretend to be a real person.[306] Users will likely see these disclosures in Facebook profiles and Twitter bios for brands using chatbots. The law prohibits chatbots from incentivizing the purchase or sale of goods and services and influencing an election vote.[307] Despite the patchwork of state and federal privacy laws, companies are still free to use AI to create user profiles, monitor user behaviors, and for other internal purposes.

2. Self-Regulation & Industry Practices

In addition to state and federal law, industry associations and government agencies develop guidelines and accepted industry standards regarding data management and governance. These guidelines are not laws, but a part of the self-regulatory framework that are considered "best practices." The self-regulatory framework has components of accountability and enforcement that regulators increasingly use as tools. Self-regulation now empowers technology companies to create standards and procedures that will hopefully have privacy concerns built into their design (i.e., privacy by design).

The FTC encourages tech companies and industry associations to develop "industry specific codes of conduct."[308] One industry group

---

[304] Disclosures must be "clear conspicuous and reasonably designed." Id.
[305] Adi Robertson, *California Just Became the First State with an Internet of Things Cybersecurity Law*, THE VERGE (Sep. 28, 2018), https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law.
[306] Adam Smith, *California Law Bans Bots from Pretending to be Human*, PCMAG (Oct. 2, 2018), https://www.pcmag.com/news/364132/california-law-bans-bots-from-pretending-to-be-human.
[307] *Id.*
[308] Federal Trade Commission, *FTC Issues Final Commission Report on Protecting Consumer Privacy,* (Mar. 26, 2012), https://www.ftc.gov/news-

helping to promote greater privacy is, the Digital Advertising Alliance (DAA), a coalition of leading industry associations.[309] Generally, these associations offer membership to organizations involved in related functions. If the associations are notified that organizations have failed to comply with the "best practices" and guidelines the association works with the organizations to become compliant. If the organization does not comply, however, the only repercussions are denying further membership opportunities.[310] Therefore, companies have no compelling incentive to follow them, other than a loss of membership.

B. European Privacy Law

Unlike the regulatory regime in the United States, the European Union's General Data Protection Regulation (GDPR) effective May 25, 2018, has some serious bite. Violators risk administrative fines up to twenty million euros or four percent of a company's worldwide annual revenue, whichever is greater.[311] As a result, tech giants such as Google have been forced to change their behavior due to sanctions under the GDPR.[312]

The difference between U.S. and EU approaches to privacy are partially due to Europe's experience in World War II. Post-war, and with the establishment of the United Nations, many countries recog-

---

events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.

[309] *Digital Advertising Regulation 101*, INTERACTIVE ADVERTISING BUREAU (Feb. 3, 2014), https://www.iab.com/news/digital-advertising-regulation-101/#4.

[310] *Id.*

[311] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[312] Google was fined $57 million by the French Data Protection Authority for failing to disclose how the company collects personal data and how the company uses it. Tony Romm, *France Fines Google Nearly $57 million for First Major Violation of New European Privacy Regime,* WASH. POST (Jan 21, 2019), https://www.washingtonpost.com/world/europe/france-fines-google-nearly-57-million-for-first-major-violation-of-new-european-privacy-regime/2019/01/21/89e7ee08-1d8f-11e9-a759-2b8541bbbe20_story.html?noredirect=on&utm_term=.0655a1c68c11.

nized that basic human rights needed to be protected to support democratic institutions.[313] In 1948, Article 12 of the Universal Declaration of Human Rights (UDHR) established principles that include privacy as a fundamental human right.[314] Article 19 provides broad protections for associated freedoms of expression.[315] The UN charter and UDHR are hortatory rather than binding law, at least in the United States.[316] However, the Council of Europe, a treaty organization consisting of all forty-seven nations in Europe, followed up with the European Convention on Human Rights (ECHR),[317] which is binding law within Europe. Balancing between privacy rights and freedom of expression is a recurring theme in European data privacy law.[318]

As a result of these different attitudes, in the EU there are privacy protections not available to those in the United States.[319] For example, personal data cannot be shared across borders without express consent from the data subject.[320] The EU developed GDPR as a regulation that is directly binding on all member states.[321] The goal was to create a coherent data protection framework with strong enforcement and enhanced rights for individuals.[322] By giving individuals more control over their data, the GDPR creates trust in the digital

---

[313] Mark Rotenberg, *On International Privacy: A Path Forward for US and Europe,* HARV. INT'L REV. (June 15, 2014), http://hir.harvard.edu/article/?a=5815.
[314] UDHR Art.12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."
[315] UDHR Art.19.
[316] Medellin v. Texas, 552 U.S. 491 (2008).
[317] Eduardo Ustaran & Hogan Lovells, European Data Protection: Law and Practice 5 (IAPP 2018) at 5-6.
[318] UDHR Art. 29(2) (articulating the principle that "In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.")
[319] Bob Sullivan, *'La Difference' Is Stark in EU, U.S. Privacy Laws,* MSN (Oct. 9, 2006), http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/#.XDGbhFxKhhE.
[320] *Id.*
[321] USTARAN, *supra* note 318 at 16 - 18.
[322] *Id.*

economy and online environment. Control, transparency, and accountability are running themes throughout GDPR.

1. Control and Consent

The GDPR gives data subjects substantially more control over their data than they previously posessed.[323] The Regulation achieves this by affording data subjects a plethora of rights,[324] including the right to object and the right not to be subject to automated decision-making.[325] This right narrowly applies when decisions are solely based on automated processing and produce legal effects regarding the data subject.[326] "As they are automated processes, AI applications are directly implicated." Subject to further regulatory guidance, this may mean AI cannot have any role in sentencing, bail, parole and other judicial decisions.[327] Data subjects would be entitled to human intervention or an opportunity to contest a decision made by AI.[328] Data subjects also have the right to receive a justification of how automated decisions are made.[329] This will cause issues for AI algorithms that are so complex that it is impossible to give data subjects an explanation of how these decisions are made.[330]

---

[323] Data subjects is contained within the definition of "personal data" as an "identified or identifiable natural person." See GDPR Art. 4(1). It is unclear whether residency in the EU is a prerequisite for protection. See GDPR Art. 4(2).

[324] *See* GDPR Art. 12-22. Data subjects' rights include the right of transparent communication and information (Art. 12-14), right of access (Art. 15), right to rectification (Art. 16), right to erasure (Art.17), right to restriction of processing (Art.18), obligation to notify recipients (Art. 19), right to data portability (Art.20), right to object (Art.21), right to not be subject to automated decision-making (Art. 22).

[325] GDPR Art. 21 & 22.

[326] USTARAN, *supra* note 317, at 166.

[327] *Id.* Regardless of these ambiguities, if decision-making processes are considered within these parameters, then processing is allowed when "authorized by law, necessary for the preparation and execution of a contract, or done with the data subject's explicit consent."

[328] *Id.*

[329] Mathias Avocats, *Artificial Intelligence and the GDPR: how do they interact?,* MATHIAS AVOCATS (Nov. 27, 2017), https://www.avocats-mathias.com/technologies-avancees/artificial-intelligence-gdpr.

[330] *Id.*

For technology companies, especially those deploying AI algorithms to mine and fuse data, consent cannot be bundled in a clickwrap, pre-ticked boxes, or by inactivity, and cannot be conditional to providing goods or services. Instead, consent must be a clear affirmative act indicating that it is freely given, specific to the various processes, and given when the person understands the full range of the use of her data.

In addition to giving data subjects broad rights, the GDPR also introduces a very high standard for "consent" when it is used by companies as a justification to process personal data. Companies must also have a lawful basis or specific, legitimate, and explicit reason to process personal data.[331] To rely on consent, companies must demonstrate that a data subject's consent was a " freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data."[332] To simplify, the EU employs an "opt-in" approach to consent, in contrast to "opt-out" consent under most U.S. laws.

2. Transparency and Accountability

European law explicitly requires processing personal data in a transparent and fair manner.[333] Repurposing data in unexpected ways can be perceived as a sinister and "creepy" threat to privacy due to complex algorithms drawing conclusions about people with unanticipated and unwelcome effects.[334] For example, a female doctor in the U.K. was locked out of a gym changing room when the automated security system profiled her as a man because it associated "Dr."

---

[331] GDPR Art. 6. "Processing" is broadly defined and has no minimum threshold, including but not limited to automatic collection, transmission, or dissemination of personal data. See GDPR Article 4.
[332] GDPR Recital 32. See Art. 7. A data subject must also be given the right to withdraw consent at any time.
[333] GDPR Art. 5(1).
[334] Information Commissioners Office, *Big Data, Artificial Intelligence, Machine Learning and Data Protection* 1, 19 (2017), https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

with males.[335] These threats also invade democratic values of equality and fairness with opaque unexplainable algorithms. Under GDPR, organizations must consider what information people have been given about the processing of their data and the consequences it could have. Generally, people are given information in privacy policies and terms of service. Because such policies are long, convoluted, and may not provide enough detail on how data will be used, companies must also consider how people reasonably expect data to be used.

The GDPR also requires accountability.[336] This is detailed in extensive record keeping obligations for organizations with at least 250 employees or when processing can risk individuals' rights or freedoms.[337] One record that must be maintained is the "purpose" for processing personal data.[338] This could pose a problem for AI and data companies who mine data for undefined purposes, or without any specific purpose in mind. Therefore, initial records will change as new data correlations are discovered prompting varying uses.

One implication of the GDPR's requirements may be to force AI to develop in an accountable and transparent manner so as to address the "black box" effect it can have. Several approaches have surfaced, including algorithmic auditing or implementing auditability into algorithm development. This would allow private companies to protect proprietary information, evaluate factors influencing algorithmic decision making, and provide public assurances. However, computation resources and technical capabilities have been cited as barriers to algorithmic audits.[339]

3. Privacy by Design

There is a developing understanding that innovation must be approached from the perspective of "Privacy by Design." This ap-

---

[335] *Id*. at 20. *See also supra* Section IV.B.2.
[336] GDPR Art. 5(2).
[337] Information Commissioners Office, *supra* note 334 at 51.
[338] GDPR Art. 30(1)(b).
[339] Information Commissioners Office, *supra note* 334 at 86.

proach incorporates privacy into technologies by 'default' at the design stage.[340] Privacy by Design is a legal requirement under GDPR[341] and a framework that propels the ideology that privacy should become an integral part of organizational priorities, objectives, development, and planning operations.[342] This framework entails that organizations default to the appropriate organizational and technical measures to ensure only necessary personal data is processed for each specific purpose.[343]

By including Privacy by Design as a legal requirement under GDPR, the EU has demonstrated privacy and data protection is a top priority for future technological developments including the use of AI. U.S. law does not ordinarily require that privacy factors be implemented into technology design or development, although the FTC encourages companies to do so voluntarily.

4. Competition Law

When it comes to using antitrust to regulate technology industries, the European Commission (the EU's antitrust enforcer) has been far more aggressive than their counterparts in the U.S. - the FTC and Department of Justice. This has implications for the regulation of data and its use in AI. Examples of aggressive EU action include the 2007 case against Microsoft in which the Commission imposed disclosure and unblocking requirements, and fined the company over €497 million, with additional fines imposed the following year as well.[344] The parallel case in the U.S. saw similar results in the Dis-

---

[340] *See, e.g.*, Intersoft Consulting, *GDPR: Privacy by Design,* https://gdpr-info.eu/issues/privacy-by-design.
[341] GDPR Art. 25.
[342] Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, PRIVACY & BIG DATA INSTITUTE, https://www.ryerson.ca/content/dam/pbdce/seven-foundational-principles/The-7-Foundational-Principles.pdf. The principles of Privacy by Design are: (1) Proactive not reactive, (2) Privacy as default, (3) Privacy embedded into design, (4) Full functionality,(5) End-to end security, (6) Visibility and transparency, and (7) Respect for user privacy.
[343] GDPR Art. 25. See Cavoukian, *supra note* 342.
[344] Microsoft v. Commission (2007) T201/04.

trict Court and Court of Appeals, with divestiture a potential remedy.[345] But before judgment President George W. Bush took office and the case was settled on meager terms.[346] U.S. antitrust enforcement has been in "a deep freeze" ever since.[347]

Anticompetitive activities by technology companies have only intensified. Facebook eliminated competition and assembled vast depositories of personal data by acquiring sixty-seven competitors. Amazon has acquired ninety-one, and Google two hundred and fourteen.[348] The Department of Justice has "allowed the almost entirely uninhibited consolidation of the tech industry into a new class of monopolists,"[349] which Columbia Law Professor Tim Wu calls the "tech trusts."[350] Meanwhile, the European Commission has taken the lead in scrutinizing American tech companies with cases against Intel,[351] Facebook,[352] Google,[353] and Qualcomm.[354] Investigations

---

[345] *See* United States v. Microsoft, 253 F.3d 34 (D.C. Cir. 2001) (discussing remedies where Microsoft was required to share its APIs with other developers, but did not have to make changes to its operating system or applications).
[346] TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE 100–01 (2018).
[347] *Id*. at 108–10 ("[A] grand total of zero anti-monopoly antitrust cases" were brought during the Bush administration, and few since).
[348] *Id*. at 123.
[349] *Id*. at 108-110.
[350] *Id*. at 118.
[351] *See* European Commission, *The Intel Antitrust Case*, http://ec.europa.eu/competition/sectors/ICT/intel.html (last visited Jan. 4, 2019) (€1.5 billion fine).
[352] *See* European Commission, *Mergers: Commission Fines Facebook €110 Million for Providing Misleading Information about WhatsApp Takeover*, http://europa.eu/rapid/press-release_IP-17-1369_en.htm (last visited Jan. 4, 2019).
[353] *See* European Commission, *Antitrust: Commission Fines Google €2.4 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service*, http://europa.eu/rapid/press-release_IP-17-1784_en.htm (last visited Jan. 4, 2019); and European Commission, Antitrust: Commission Fines Google €4.34 Billion for Illegal Practices Regarding Android Mobile Devices to Strengthen Dominance of Google's Search Engine, http://europa.eu/rapid/press-release_IP-18-4581_en.htm (last visited Jan. 4, 2019).
[354] *See* European Commission, *Antitrust: Commission Fines Qualcomm €997 Million for Abuse of Dominant Market Position*, http://europa.eu/rapid/press-release_IP-18-421_en.htm (last visited Jan. 4, 2019).

of Amazon and Apple are underway.[355] Ironically, many of the complainants before the Commission are other U.S. companies who do not feel that U.S. regulators adequately protect competition.

The Commission is now going beyond traditional antitrust law and "taking a hard look at an increasingly important corporate currency: data."[356] It "is not the amount of money at stake, but the amount of data"[357] they can exploit that is under scrutiny. Competition Commissioner Margrethe Vestager has "emerged as a major voice of warning about the effect of tech firms on our habits, our privacy, our ability to make human connections and even democracy itself."[358] Coupled with its new privacy regime, this push back by the EU could threaten the global dominance of American technology companies. Along these lines, Germany's Cartel Office recently prohibited Facebook from aggregating data with its third-party services without voluntary consent of its users.[359] One Canadian official has gone farther, suggesting that the company be broken up.[360] At the very least, discontinuity among the various competition and privacy regimes imposes significant economic and social uncertainty. Perhaps in response, the FTC has begun to focus on "the consequences

---

[355] *See* Aoife White, *After Google, EU's Antitrust Sights May Turn to Amazon and Apple*, https://www.bloomberg.com/news/articles/2019-03-20/after-google-eu-s-antitrust-sights-may-turn-to-amazon-and-apple.
[356] Natalia Drozdiak, *EU ASKS: Does Control of "Big Data" Kill Competition?*, WALL ST. J. (Jan. 2, 2018), https://www.wsj.com/articles/eu-competition-chief-tracks-how-companies-use-big-data-1514889000.
[357] Sarah Lyall, *Who Strikes Fear Into Silicon Valley? Margrethe Vestager, Europe's Antitrust Enforcer*, N.Y. TIMES (May 5, 2018), https://www.nytimes.com/2018/05/05/world/europe/margrethe-vestager-silicon-valley-data-privacy.html.
[358] *Id.*
[359] *See Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources*, BUNDESKARTELLAMT (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.
[360] *See* Romm, *supra* note 173.

of having differing approaches internationally to competition, consumer protection, and privacy enforcement around artificial intelligence and other emerging technologies."[361]

Monopoly power permits tech behemoths to distort marketplaces in other ways. First, is the market for talent in the knowledge economy. Data scientists, roboticists and AI engineers, some commanding million-dollar salaries,[362] are gobbled up by tech companies in an AI arms race.[363] This has "thinned out top academic departments,"[364] and led to vacuums in other industries,[365] increasing wage inequality and exacerbating housing crises in Silicon Valley and other technology centers.[366] Second, these companies have relatively low costs of production relative to the market prices of their

---

[361] *See FTC Hearing #11: The FTC's Role in a Changing World, Hearings on Competition and Consumer Protection in the 21st Century*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/events-calendar/ftc-hearing-11-competition-consumer-protection-21st-century.

[362] Gideon Lewis-Kraus, *The Great AI Awakening*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html (Mark Zuckerberg "personally oversees, with phone calls and video-chat blandishments, his company's overtures to the most desirable graduate students. Starting salaries of seven figures are not unheard-of"). *See also* Cade Metz, *AI Researchers Are Making More Than $1 Million, Even at a Nonprofit*, N.Y. TIMES (April 19, 2018), https://www.nytimes.com/2018/04/19/technology/artificial-intelligence-salaries-openai.html ("AI specialists with little or no industry experience can make between $300,000 and $500,00 a year in salary and stock.").

[363] *Id*. The demand for AI engineers is so intense that Silicon Valley tech companies entered into a mutual "non-poaching" agreement. Both the Department of Justice and a class of engineers filed antitrust actions. *See In re* High Tech Employee Antitrust Litigation, Case No. 11-CV-2509-LHK (N.D. Cal. 2015); *see also* Matt Phillips, *Apple's $1 Trillion Milestone Reflects Rise of Powerful Megacompanis,* N.Y. TIMES (Aug. 2, 2018), https://www.nytimes.com/2018/08/02/business/apple-trillion.html.

[364] Lewis-Kraus, *supra* note 362.

[365] *Id.*

[366] *See* Richard Waters, *The Great Silicon Valley Land Grab*, FIN. TIMES (Aug. 25, 2017), https://www.ft.com/content/82bc282e-8790-11e7-bf50-e1c239b45787. Also, due to uncertainty in immigrant visas, many tech companies are moving some of their AI operations to Canada. Gene Marks, *Canada's Tech Companies Are Benefiting From Tightening U.S. Immigratio*n, WASH. POST (Apr. 12, 2018), https://www.washingtonpost.com/news/on-small-business/wp/2018/04/12/canadas-tech-companies-are-benefiting-from-tightening-u-s-immigration/?utm_term=.3e987d0fcba1.

products. While this spurred a bull market after the end of the Great Recession,[367] the benefits are not equally shared by other sectors, possibly depressing investment there.[368]

Finally, AI has fueled the concentration of power by technology and platform companies[369] that is "partially independent of states as well as international political institutions."[370] Because of their market dominance, they can and do displace traditional law with "terms of service" rules that act as separate legal systems.[371] "While Mark Zuckerberg mused recently that Facebook might need an analog to the Supreme Court to adjudicate disputes and hear appeals, Amazon already has something like a judicial system—one that is secretive, volatile, and often terrifying."[372] A growing industry of consultants operates in place of lawyers, helping Amazon sellers appeal algorithmically-based decisions to demote or suspend their products.[373] Dominance of this scope undermines free market principles and democracy. Regulators must take greater notice of these concentrations of power, lest the term "sovereign state of Facebook" become more than simply a metaphor.[374]

C. Regulating Robots and AI

---

[367] Phillips, *supra* note 363.
[368] Matt Phillips, *Apple's $1 Trillion Milestone Reflects Rise of Powerful Mega-companis*, N.Y. TIMES (Aug. 2, 2018), https://www.nytimes.com/2018/08/02/business/apple-trillion.html.
[369] *See, e.g.,* Liu, *supra* note 22 (arguing that the concentration of power in "military institutions and private corporations [that] currently drive AI research and development, potentially distort[] notions of democratic and civilian control.").
[370] Ünver, *supra* note 7 at 2.
[371] *See* Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328, 356-357 (2018) ("Facebook's own content rules and terms of service … may be more influential in shaping speech on the platform than any one state's law").
[372] Josh Dzieza, *Prime and Punishment; Dirty Dealing in the $175 Billion Amazon Marketplace*, THE VERGE (Dec. 19, 2018), https://www.theverge.com/2018/12/19/18140799/amazon-marketplace-scams-seller-court-appeal-reinstatement.
[373] *Id*.
[374] *See* Molly Roberts, *Facebook Has Declared Sovereignty*, WASH. POST (Jan. 31, 2019), https://www.washingtonpost.com/opinions/2019/01/31/facebook-has-declared-sovereignty; Kate Klonick, *The New Governors: The People, Rules, And Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1617, n. 125 (2018) (collecting literature discussing "feudal" and "sovereign" platforms).

1. Law of the Horse

In the 1990s, as the internet was gaining traction, Frank Easterbrook and Lawrence Lessig had a public colloquy on the need for a new legal discipline and regulation for cyberspace. Judge Easterbrook argued that law schools no more needed a course on cyberlaw than they needed a course on the "law of the horse" to deal uniquely with equine issues.[375] Professor Lessig had the contrary view; that specific attention was needed to "how law and cyberspace connect."[376] In the two decades since their debate, Lessig's view has prevailed as the internet has impacted every facet of law.[377] Ryan Calo subsequently applied Lessig's approach and his later theory that "code is law" to the field of robotics.[378]

Lessig has described two different regulatory paradigms for the internet: "East Coast Code" and "West Coast Code." The former is the familiar government control by statute or agency regulation.[379] The latter is the architecture of the internet; namely how the software code that runs the internet (and other technologies) is itself a regulatory tool. Engineers can supplement or displace legal regulation by their software designs.[380]

The Easterbrook-Lessig debate over internet regulation is being replicated with AI. Some think that the beast can be tamed by adapting "existing rules on privacy, discrimination, vehicle safety and so on" to AI.[381] We take the other road and argue for a "law of the AI

---

[375] Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207.
[376] Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 502 (1999).
[377] "Internet exceptionalism" has become a popular discourse in legal literature. *See, e.g*., Mark Tushnet, *Internet Exceptionalism: An Overview From General Constitutional Law*, 56 WM. & MARY L. REV. 1637 (2015); Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CAL. L. REV. 513, 551-52 (2015).
[378] *Id.* at 559. *See also* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).
[379] *Id.* at 53.
[380] *Id*. at 60.
[381] Tom Standage, *There Are No Killer Robots Yet—But Regulators Must Respond To AI In 2019*, ECONOMIST (Dec. 17, 2018), https://www.economist.com/the-world-in/2018/12/17/there-are-no-killer-robots-yet-but-regulators-must-respond-to-ai-in-2019. For another thoughtful discussion, see Heidi Vogt,

horse;" or laws specifically directed to the use of AI in modern life. Until regulators move to control misuses of AI and robots, the technologies will be governed by the code their developers build into them. As described earlier in this Article, currently the design of AI software allows for profound misuse. While this software may not be specifically designed to undermine privacy or obstruct democratic processes, there is a risk it could be. As the GDPR and the EU's proposed laws on robotics demonstrate, regulations must take this into account.

2. Proposed EU Laws on Robotics

Following a report from its Legal Affairs Committee, the European Parliament in 2017 sent a request to the European Commission seeking the development of "Civil Law Rules on Robotics" for the European Union.[382] The Commission published a preliminary response agreeing with many of the Parliament's concerns, including AI's "socio-economic impact as well as its consequences on the rule of law, fundamental rights and democracy."[383] A consultation with the public followed that tracked those concerns, emphasizing the protection of EU values (like privacy and data protection), , and the need for liability rules, and better enforcement of adopted regulations.[384]

Should the Government Regulate Artificial Intelligence, WALL ST. J. (Apr. 30, 2018), https://www.wsj.com/articles/should-the-government-regulate-artificial-intelligence-1525053600.

[382] EUR. PARL. DOC. P8_TA (2017)0051, *Civil Law Rules on Robotics: European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics*, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//EN. Most EU legislation is initiated by the Commission.

[383] *Follow up to the European Parliament resolution of 16 February 2017 on civil law rules on robotics*, European Commission. The Commission has adopted or is developing several legislative initiatives on AI. These include The Machinery Directive 2006/42/EC, the "Better Regulation Package" to assess impacts on fundamental rights, and an investigation into IoT and autonomous system liability. *Id.*

[384] *See* http://www.europarl.europa.eu/cmsdata/130181/public-consultation-robotics-summary-report.pdf (last visited Jan. 4, 2019).

The Parliament's proposal for new laws and policies include[385]:

- codifying Isaac Asimov's three laws of robotics;[386]
- creation of liability rules for robot harms and accountability for AI engineers;
- registration and classification of AI systems to facilitate traceability and control;
- development of ethical principles, including a code of conduct for AI engineers, based on beneficence, non-maleficence, human autonomy and justice;
- mitigation of risk to human safety, health and security, freedom, privacy, integrity and dignity, self-determination, non-discrimination and personal data protection;
- mandated transparency and explainability, including recordation of all steps taken by AI that contribute to its decisions;
- use of open source code in design and interoperability of autonomous robots; and
- the creation of a European Agency for Robotics and Artificial Intelligence to both promote and regulate developing technologies.

Such policies could go a long way toward abating the risks identified in this Article, many of which are also reflected in the Parliament's proposal.[387] It may be that if EU rules are adopted they could have

---

[385] EUR. PARL. Res. 2015/2103(INL), *Report with Recommendations to the Commission on Civil Law Rules on Robotics,* http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2017-0005&language=EN.

[386] The "laws" first appeared in the short story *Runaround* in ISAAC ASIMOV, ASTOUNDING SCIENCE FICTION (1942), and have appeared in nearly every science and science fiction story about robots since then. They are: 1) "A robot may not injure a human being or, through inaction, allow a human being to come to harm;" 2) "A robot must obey the orders given it by human beings except where such orders would conflict with the First Law;" and 3) "A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws."

[387] *Id*. at G (AI presents "not only economic advantages but also a variety of concerns regarding [its] direct and indirect effects on society as a whole"); H ("rais[es] challenges to ensure non-discrimination, due process, transparency and understandability in decision-making processes").

extraterritorial effect on AI development in the United States and elsewhere outside of Europe. That is what functionally has happened with GDPR. All U.S. tech companies and many smaller firms need to comply with EU privacy rules as a condition of participating in trans-Atlantic business, thus filling the void in U.S. privacy law. Even as large tech companies further insert AI into our public and private lives, they may be forced to respect the democracy reinforcing principles enshrined in Europe's AI laws if and when those laws are enacted.

The United States was not always so far behind. In 2014 and 2016, the President's Council of Advisors on Science and Technology (PCAST) and the National Science and Technology Council (NSTC) issued several reports on big data and privacy.[388] The NSTC also issued white papers such as *AI: Preparing for the Future of Artificial Intelligence*,[389] and *The National Artificial Intelligence Research and Development Strategic Plan*.[390] While these were frameworks rather than specific policy proposals, they did raise concerns about the "unintended consequences" of AI, especially in areas of "justice, fairness, and accountability."[391] These plans were important first steps and might have led to addressing "complex policy challenges related to the use of AI."[392] But those plans have been mostly abandoned.[393] Instead, current strategies on big data and AI

---

[388] *See* Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, May 2014, https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.; Executive Office of the President: *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, May 2016, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

[389] Executive Office of the President, *Preparing for the Future of Artificial Intelligence,* October 2016, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

[390] Executive Office of the President, *The National Artificial Intelligence Research and Development Strategic Plan*, October 2016, https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf.

[391] Preparing for the Future, *supra* note 389, at 30.

[392] AI Strategy, *supra* note 390, at 7.

[393] PWC, supra note 132 at 19. Measured by the number of peer-reviewed papers, academic interest in AI has grown 8-fold since 1996, but most of that increase is occurring in Europe and China, rather than the U.S., which has fallen to

focus on promoting their uses and removing regulatory barriers, rather than mitigating risks.[394]

3. Asilomar Principles

Ideas for how to regulate AI need not come only from government. Civil society can also play an important role. A growing and global "responsible AI" movement[395] comprised of non-governmental organizations, scholars, and scientists have lately begun to take up the public interest challenges posed by AI.[396] A group including Elon Musk,[397] Bill Gates, and the late Stephen Hawking, issued an "Open Letter on Artificial Intelligence" in 2015, subsequently signed by over 8,000 AI and policy researchers.[398] The Letter affirmed that AI "has the potential to bring unprecedented benefits to humanity," but also warned of "potential pitfalls,"[399] among which were threats to privacy, ethical norms and human control.[400] This was followed by

---

third place. *See AI Index*, *supra* note 17, at 8-10. This is reflected in the comparative growth in AI patents issued. *Id*. at 35. On February 11, 2019, President Trump issued Executive Order 13859, "Maintaining American Leadership in Artificial Intelligence," which may have been in response to China's "Made in China 2025" goal of capturing the lead in AI and quantum computing. A secondary goal is to increase public trust in AI technologies and protect "civil liberties, privacy and American values."

[394] *See*, *e.g*., Whitehouse, Artificial Intelligence for the American People, at https://www.whitehouse.gov/briefings-statements/artificial-intelligence-american-people; National Big Data R&D Initiative at https://www.nitrd.gov/nitrdgroups/index.php; Artificial Intelligence R&D Interagency Working Group, id.

[395] PWC Report, supra note 132.

[396] *See, e.g*., NYU's AI Now Institute, https://ainowinstitute.org; Harvard's Ethical Machine, https://ai.shorensteincenter.org.

[397] Musk also co-founded OpenAI, a non-profit research company working on creating safe and "friendly" AI. Its principal work is in AI engineering, but subscribes to the theory described above that "West Coast Code," i.e., the architecture of autonomous machines, should be designed to avoid harms to humanity or undue concentrations of power. See https://blog.openai.com/openai-charter.

[398] *See An Open Letter: Research Priorities for Robust and Beneficial Artificial Intelligence*, FUTURE OF LIFE INSTITUTE, https://futureoflife.org/ai-open-letter (last visited Jan. 4, 2019).

[399] Stuart Russell, Daniel Dewey, Max Tegmark, *Research Priorities for Robust and Beneficial Artificial Intelligence,* AI Magazine, Winter 2015, at 112, https://aaai.org/ojs/index.php/aimagazine/article/view/2577.

[400] *Id*. at 107.

a set of principles developed at the Asilomar Conference on Beneficial AI in January 2017.[401]

The Asilomar principles correspond to and inform the recommendations we make here. The values that AI and their developers should adhere to include: liberty, privacy, responsibility, judicial transparency, and respect for human dignity. One other principle is vitally important: "The power conferred by control of highly advanced AI systems should respect and improve, rather than subvert, the social and civic processes on which the health of society depends."[402]

The Asilomar principles lend moral authority and competency to questions that the other two rails of society – government and business – have thus far neglected. In late 2018, the California Legislature formally adopted the Asilomar Principles.[403] Perhaps this will start a trend.

4. Recommendations

The lack of privacy online and in physical spaces is so pervasive that many Americans have reconciled themselves to the view expressed by Sun Microsystem CEO Scott McNealy: "you have zero privacy anyway. Get over it."[404] Hopefully, most Americans reject that view, as we do. If Congress were to get serious about modernizing privacy law, quite apart from the impact that social media and AI are having, it might consider the following proposals:[405]

- treat information privacy as a fundamental human right;[406]

---

[401] *See Asilomar AI Principles*, FUTURE LIFE INST., https://futureoflife.org/ai-principles. The Asilomar conference was sponsored by the Future of Life Institute..

[402] *See Asilomar AI Principles*, ARTIFICIAL INTELLIGENCE BLOG, https://www.artificial-intelligence.blog/news/asilomar-ai-principles (last visited Jan. 4, 2019).

[403] Assemb. Con. Res. 215, 2017-18 Leg. (Cal. 2018).

[404] Polly Springer*, Sun on Privacy: Get Over It*, WIRED (Jan. 26, 1999), http://www.wired.com/1999/01/sun-on-privacy-get-over-it.

[405] We recognize that this is a wish list of regulatory reform. But, at some point, something akin to these will need to be enacted if we are to preserve core values.

[406] Universal Declaration of Human Rights, Art.12, available at http://www.un.org/en/universal-declaration-human-rights/: "No one shall be

- require privacy by design and incentivize technology companies to be privacy conscious;[407]
- adopt opt-in models (rather than opt-out) for consent and authorization as Europe does under the GDPR;
- require full transparency on the downstream uses of user data; [408]
- impose liability for unconsented collection, use or trafficking; and
- recognize ownership, control and choice of personal data by "data subjects."[409]

Many of the above measures could be accomplished by adopting regulations similar to GDPR or CCPA. But the growing use of AI in the data ecosystem requires that Congress go further. It should also:

- enact legislation that requires articulable and specific privacy processes, cybersecurity standards, and anonymity procedures with statutory penalties for violations and private rights to action;
- subject IoT, data aggregation, fusion and analytics to regulatory oversight and third-party auditing requirements;
- promote blockchain or similar chain-of-title technology to allow users to take ownership of their data and monetize its use; and
- require human supervision and accountability for algorithmic use of PII and any information related to or that has the potential to relate to a person, including transparent justification for automated decisions.[410]

---

subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Every-one has the right to the protection of the law against such interference or attacks."

[407] Derek Care, International Association of Privacy Professionals: Privacy, Security, Risk Conference (Oct 19, 2018)..

[408] GDPR Art. 5(1) (providing that data should be processed in a transparent and fair manner).

[409] This is, functionally, the approach taken by the GDPR insofar is it gives European residents the right to control collection, use and disclosure of their personal data.

[410] *See supra* Section IV.B.2.

Protecting democratic values and institutions from the risks posed by AI will also require serious attention and legislation. "East Coast Code" (formal law) will eventually develop. It could be anemic and industry oriented, as federal privacy law has turned out to be. Or public dissatisfaction with AI abuses could prompt a comprehensive regulatory scheme along the lines of the European Parliament's proposal. An AI regulatory regime would optimally include at least the following features:[411]

- transparency, accountability, and responsibility for AI design and processes;[412] transparency of and access to training and operational data;[413]
- reproducibility of results by disinterested agents;[414]
- override of the "third party" and "state action" doctrines and intentionality requirement for constitutional challenges to AI functions and privacy violations;[415]

---

[411] To the extent legislatures are responding to the challenges of AI, it is usually with liability rules. However, in California, a state oversight body has recently issued recommendations similar to those contained here. See *Artificial Intelligence: A Roadmap for Californi*a, Little Hoover Commission 14 (Nov. 2018).

[412] This and several other recommendations here may require that control code of AI systems be "open source," rather than proprietary. This would undermine trade secret law unless that too were modified, such as by exempting disclosures under regulatory requirements. Patent law could also be liberalized to incentivize and protect AI inventions

[413] A similar problem arises here since source, training and test data is typically kept confidential to preserve its economic value. In response to disclosure mandates, data could be given property-like rights, rather than relying on trade secret for protection. *See generally* Jeffrey Ritter and Anna Mayer, *Regulating Data As Property*, 16 DUKE L. & TECH. REV. 220 (2018).

[414] Opaqueness in AI processing, especially with Deep Learning, leads to unexaminable outputs. *See supra* notes 245-247 and accompanying text. Third-party reproducibility at least allows for external testing of outputs.

[415] The state action doctrine precludes the assertion of constitutional claims against private parties in most cases. *Supra* note 238. Yet, it is the private owners of AI technologies that are apt to do the most damage to constitutional rights. While it would be difficult for Congress to extend the constitution to third parties, it could create parallel statutory rights that bind them. *See, e.g.,* Civil Rights Act of 1964, 78 Stat. 241. The third-party doctrine is judicially created and can be modified either by Congress or the Supreme Court.

- enforcement of ethical principles for those involved in the design, development and implementation of AI;[416]
- openness in AI development, systems and databases;[417]
- non-delegation to autonomous actors of decisions affecting fundamental rights;[418]
- limiting "safe harbor" immunity under the Communications Decency Act and Digital Millennium Copyright Act for large internet platforms that fail to take technologically feasible steps to curb disinformation campaigns;[419]
- limitations on the market power of AI companies, including divestiture where appropriate;[420] and
- two laws added to Asimov's trilogy: primacy of human well-being and values; and full disclosure by autonomous actors.[421]

While these recommendations do not fully resolve AI's risks, we believe they provide a framework, at least for further discussion.

---

[416] MIT recently announced a new college of computing and AI, emphasizing "teaching and research on relevant policy and ethics" of AI. See MIT News Office, *MIT Reshapes Itself to Shape the Future*, MIT NEWS (Oct. 5, 2018), http://news.mit.edu/2018/mit-reshapes-itself-stephen-schwarzman-college-of-computing-1015.

[417] *See* Nick Bostrom, *Strategic Implications of Openness in AI Development, GLOBAL POL'Y* (2017), https://nickbostrom.com/papers/openness.pdf. Market dominance threatens privacy and democratic values for the reasons discussed in section V(b)(4).

[418] We explain in the text accompany *supra* notes 247-250, how autonomous decision-making can mask constitutional violation, erode due process, and preclude meaningful judicial review. It also degrades human integrity by subjecting fundamental rights to algorithmic control. A rule limiting delegation to machines is necessary to avoid "algocracy."

[419] *See* supra note 183. Lazar et al propose a collaboration between social media platforms and the scientific community to design effective interventions to combat fake news. The industry has resisted this so far, fearing that it could lead to regulation. *Id*. at 1096.

[420] *See* Wu, *supra* note 346 (arguing that concentration of power in giant firms threatens democracy).

[421] Asimov himself had proposed a "zeroth law" that would prioritize protection of humanity above all other robot obligations. Isaac Asimov, *Robots and Empire* (1985). Our second suggestion incorporates Marc Rotenberg's proposed "fourth" and "fifth" laws – robot identification and explanation. *See* Marc Rotenberg, *Privacy in the Modern Age: The Search for Solutions*, EPIC (Oct. 19, 2016), https://epic.org/privacy/intl/EPIC-38ICDPPC-kyn-10-16.pdf.

Yet, we are not optimistic about them being adopted in the near term. Given the current trajectory of power dominance by large tech companies, not only over AI but over our democratic institutions as well, it may take a major event or systemic reconfiguration for that to occur. But with the steep curve in AI development, and the public disaffection exhibited around the globe with the status quo, we may be in for a surprise. As Bill Gates reminds us, "we always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten."[422] That applies both to the prospect for reform and to AI itself. Without a national dialogue and legislative action of some form, a decade from now privacy and democracy could exist mostly in our memory.

CONCLUSION

The Economist Intelligence Unit publishes a "Democracy Index" each year gauging the state of democracy around the world.[423] For 2017 it found that over half of the countries surveyed experienced a decline in their democracy "scores." Principal factors are: declining participation in elections, weakness in the functioning of government, declining trust in institutions, erosion of civil liberties, decline in media freedoms, and growing influence of unaccountable institutions. On the basis of this scoring, the United States was demoted from a "full democracy" to a "flawed democracy." The study noted that "erosion of confidence in government and public institutions" is especially problematic in the U.S.[424] This Article posits that the

---

[422] BILL GATES, THE ROAD AHEAD 316 (1995). This is a restatement of Amara's Law ("We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run").

[423] Economist Intelligence Unit, *Democracy Index 2017: Free Speech Under Attack*, ECONOMIST INTELLIGENCE UNIT (last visited Aug. 10, 2018) http://pages.eiu.com/rs/753-RIQ-438/images/Democracy_Index_2017.pdf. This is a sister publication to the Economist magazine.

[424] *Id.* at 20. The 2018 Democracy Index saw continued deterioration in scores, despite increased electoral participation by women. The U.S. fell further behind and remains a "flawed democracy." Economist Intelligence Unit, *Democracy Index 2018: Me Too?: Political Participation, Protest And Democracy* 10, ECONOMIST INTELLIGENCE UNIT (last visited April 22, 2019), https://www.prensa.com/politica/democracy-index_LPRFIL20190112_0001.pdf.

increasing deployment of artificial intelligence is at least partly to blame for this trend.

We have focused on two intertwined areas where AI contributes to the disaffection: privacy and democracy. AI is not itself the culprit. As a technology, it is no more inherently bad than, say, electricity. Rather it is how the tool is used, by whom, and for what purpose that generate concern. Those who would profit economically or ideologically from the erosion of rights tend to be the ones who exploit the capabilities of AI in a weak regulatory environment.[425] Thus, "surveillance capitalism" prospers because privacy rights are grossly underprotected and our laws have failed to keep pace with technology. Our last major federal privacy law (ECPA) was enacted in 1986, before Facebook, before Google and YouTube, indeed before the World Wide Web. Data and AI companies have grown and flourished in the interim, now commanding disproportionate power over the economy, public policy, and our lives.

There are no comprehensive federal laws dealing with AI. In their absence, industry self-regulation, and awareness are the best we can hope for. And while many in the AI community, including at major technology companies, share the concerns expressed here, the quest for market dominance has thus far outweighed ethics and rights.

This is a problem that has been brewing for decades. The advent of social media and the industry's disregard for user privacy has simply made matters worse, often with the assistance of smart algorithms. The situation will likely get even worse as the "tech trusts" develop stronger and more pervasive AI. The "high levels of social control" that AI enables may herald a "coming competition between digital authoritarianism and liberal democracy."[426]

AI is also the favorite tool of foreign powers and political hackers to influence elections in the United States and abroad. Despite the Russia and Cambridge Analytica scandals, little is being done to abate what appear to be permanent risks. According to FBI Director

---

[426] Wright, *supra* note 1.
[426] Wright, *supra* note 1.

Christopher Wray, "this is not just an election cycle threat. Our adversaries are trying to undermine our country on a persistent and regular basis."[427]

Some scientists, philosophers and futurists have sounded alarms about the existential threat that AI and autonomous robots pose to humanity.[428] We do not go nearly that far. But it seems inescapable that AI is having a profound effect on constitutional rights and democratic institutions. As Harari notes:

Artificial intelligence could erase many practical advantages of democracy, and erode the ideals of liberty and equality. It will further concentrate power among a small elite if we don't take steps to stop it.[429]

We may not need to stop AI, but we certainly need to pay attention. "The way in which regulation is put in place is slow and linear, [yet] we are facing an exponential threat [from AI]. If you have a linear response to an exponential threat, it's quite likely that the exponential threat will win."[430]

In this Article, we have discussed the risks of AI with the assumption that democratic ideals are foundational to society and should be protected. But, of course, that is not true everywhere. Many authoritarian regimes do not agree with our premise. For them, AI is a marvelous tool to strengthen control of their people. China, for one, is perfecting the use of AI to increase surveillance.[431] The "China Brain Project" uses deep learning to amass information about online

---

[427] FBI Director Christopher Wray's Statement at Press Briefing on Election Security, Aug. 2, 2018, https://www.fbi.gov/news/pressrel/press-releases/fbi-director-christopher-wrays-statement-at-press-briefing-on-election-security.
[428] *See, e.g.*, Bostrom, *supra* note 15; Liu, *supra* note 22.
[429] Yuval Harari, *Why Technology Favors Tyranny*, ATLANTIC (Oct. 2018), https://www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330.
[430] *Elon Musk: Humans Must Merge with Machines,* AXIOS (Nov. 26, 2018), https://www.axios.com/elon-musk-humans-must-merge-with-machines-1543240787-c51eee35-8cb3-4684-8bb3-7c51e1327b38.html.
[431] *See, e.g.*, Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*, N.Y. TIMES (July 8, 2018), https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

and offline user behavior.[432] The resulting "social credit system"[433] takes data collection, fusion and analytics to a new level. Perhaps it is not surprising that the Chinese government is outspending the U.S. government in AI research,[434] with the aim of setting global standards for AI.[435] For the United States to retake the lead, it will first have to address the very real risks to privacy and democracy discussed here. Otherwise, we risk going the way of China.[436]

---

[432] *See* Ünver, *supra* note 7 at 7.

[433] *See* State Council Notice Concerning Issuance of the Planning Outline for the Establishment of a Social Credit System (2014-2020) (translation), https://www.chinalawtranslate.com/socialcreditsystem (last visited Jan. 5, 2019).

[434] *See* Christina Larson, *China's Massive Investment in Artificial Intelligence Has an Insidious Downside*, SCIENCE (Feb. 8, 2018), https://www.science-mag.org/news/2018/02/china-s-massive-investment-artificial-intelligence-has-insidious-downside.

[435] *See* China State council's "New Generation Artificial Intelligence Development Plan," described in Graham Webster et al., *China's Plan to 'Lead' in AI: Purpose, Prospects, and Problem*s, https://www.newamerica.org/cybersecurity-initiative/blog/chinas-plan-lead-ai-purpose-prospects-and-problems (last visited Jan. 5, 2019).

[436] *See* Farhood Manjoo, *It's Time to Panic About Privacy*, N.Y. TIMES (Apr. 10, 2019), https://www.nytimes.com/interactive/2019/04/10/opinion/internet-data-privacy.html ("Here is the stark truth: We in the West are building a surveillance state no less totalitarian than the one the Chinese government is rigging up").