ARTIFICIAL INTELLIGENCE AND PRIVACY

by

Daniel J. Solove

Draft: February 1, 2024

ABSTRACT

This Article aims to establish a foundational understanding of the intersection between artificial intelligence (AI) and privacy, outlining the current problems AI poses to privacy and suggesting potential directions for the law's evolution in this area. Thus far, few commentators have explored the overall landscape of how AI and privacy interrelate. This Article seeks to map this territory.

Some commentators question whether privacy law is appropriate for addressing AI. In this Article, I contend that although existing privacy law falls far short of addressing the privacy problems with AI, privacy law properly conceptualized and constituted would go a long way toward addressing them.

Privacy problems emerge with AI's inputs and outputs. These privacy problems are often not new; they are variations of longstanding privacy problems. But AI remixes existing privacy problems in complex and unique ways. Some problems are blended together in ways that challenge existing regulatory frameworks. In many instances, AI exacerbates existing problems, often threatening to take them to unprecedented levels.

Overall, AI is not an unexpected upheaval for privacy; it is, in many ways, the future that has long been predicted. But AI glaringly exposes the longstanding shortcomings, infirmities, and wrong approaches of existing privacy laws.

Ultimately, whether through patches to old laws or as part of new laws, many issues must be addressed to address the privacy problems that AI is affecting. In this Article, I provide a roadmap to the key issues that the law must tackle and guidance about the approaches that can work and those that will fail.

ARTIFICIAL INTELLIGENCE AND PRIVACY

By Daniel J. Solove[1]

[1] Eugene L. and Barbara A. Bernard Professor of Intellectual Property and Technology Law, George Washington University Law School.

INTRODUCTION

> When art and science meet in wond'rous guise,
> And machines take on a mind of their own,
> There is a fear that fills our hearts and eyes,
> That privacy, once cherished, shall be gone.
>
> - ChatGPT

Artificial intelligence (AI) is in the midst of a magical moment. AI is everywhere, and everyone seems to be talking about it. As AI rapidly advances around the world and barges into nearly every facet of life, it raises a host of problems, from intellectual property to employment to safety, among others, including privacy. Further complicating the situation, AI affects privacy in many different ways and raises a multitude of concerns.

In this Article, I aim to lay the conceptual and practical groundwork for how to understand the relationship between AI and privacy as well as provide a roadmap for how privacy law should regulate AI. Thus far, few commentators have explored the overall landscape of how AI and privacy interrelate. This Article seeks to map this territory.

Existing privacy laws already address AI to some extent, such as the European Union's General Data Protection Regulation (GDPR), which has a few provisions devoted to "automated" data processing.[2] Several U.S. state consumer privacy laws also have provisions on automation, though they are narrow and limited.[3] New laws focused exclusively on AI are on the horizon. The EU recently enacted the AI Act.[4] AI laws are starting to germinate in the U.S.[5]

Is privacy law the appropriate tool to regulate these issues? Or are AI's privacy issues best regulated by specialized AI laws? Some commentators question whether privacy law is appropriate for addressing AI. As law professor Eric Goldman argues:

> To privacy advocates, an ever-expanding scope for privacy law might sound like a good thing. For the rest of us, it's unquestionably not a good thing. We don't want privacy experts making policy decisions about topics outside their swimlanes. They lack the requisite expertise, so they will make serious

[2] GDPR art. 22.

[3] *See infra* at X.

[4] EU Parliament, *Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI,* Dec. 9, 2023, https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai.

[5] National Conference of State Legislatures, Artificial Intelligence 2023 Legislation (Jan. 12, 2024), https://www.ncsl.org/technology-and-communication/artificial-intelligence-2023-legislation.

and avoidable policy errors.[6]

In this Article, I contend that although existing privacy law falls far short of addressing the privacy problems with AI, privacy law properly conceptualized and constituted would go a long way toward addressing them.

To determine how the law ought to regulate AI and privacy, several fundamental matters must be examined and explained. First, it is essential to understand what AI is. This matter is complicated because what is called "AI" today is not what the term has long meant in common understanding, which has been sentient robots. The term "AI" is now being used to describe machine learning algorithms and related technologies, and they are not the same as machines that can think for themselves. Today's AI is, quite interestingly, both old and new, a step in a long evolution but also a significant leap forward. Much of today's AI technologies are well-known to privacy law, and the ways they affect privacy are hardly surprising.

Second, the privacy problems raised by AI must be understood. To determine how the law should regulate, where existing law falls short, and what changes or additions should be made to the law, an understanding of the big picture is crucial. AI involves algorithms that consume inputs and produce outputs. Privacy problems emerge with both inputs and outputs. These privacy problems are often not new; they are variations of longstanding privacy problems.[7] But AI remixes existing privacy problems in complex and unique ways. Some problems are blended together in ways that challenge existing regulatory frameworks. In many instances, AI exacerbates existing problems, often threatening to take them to unprecedented levels.

Problems with inputs involve problems with data collection, which include scraping (the non-consensual gathering of data online) as well as more consensual forms of data collection. Both forms of data collection are poorly addressed by most privacy laws.

The privacy problems with AI's outputs involve data generation, decision-making, and data analysis. New data generated by making inferences can reveal details about people that they don't expect and don't want to reveal. Data generation blurs the line between data collection and data processing, allowing end-runs around many privacy law protections.

AI data generation can also produce malevolent material at an unprecedented scale, which can exacerbate problems involving deception and manipulation and

[6] Eric Goldman, *Privacy Law Is Devouring Internet Law (and Other Doctrines)…To Everyone's Detriment,* Technology & Marketing Law Blog (May 9, 2023), https://blog.ericgoldman.org/archives/2023/05/privacy-law-is-devouring-internet-law-and-other-doctrines-to-everyones-detriment.htm.

[7] I have previously developed an extensive taxonomy of the many different yet related privacy problems. *See* Daniel J. Solove, *A Taxonomy of Privacy,* 154 U. Pa. L. Rev. 477 (2006).

create new data security vulnerabilities. Even non-malevolent AI content can be deceptive and manipulative, such as when AI simulates humans in certain circumstances.

Another set of AI outputs involves the use of AI algorithms to make decisions about people. AI can make predictions about people's future behavior, which can lead to interventions and judgment for things people haven't yet done, diminishing respect for human agency. Automation in AI decision-making depersonalizes it, skewing it toward quantifiable dimensions and away from non-quantifiable unique details about people. AI can also systematically encode bias into decisions.

Additionally, AI data analysis can magnify privacy-invasive practices such as surveillance and identification, enhancing the power and control of the watchers.

AI raises vexing challenges for regulatory oversight, stakeholder participation, and accountability. AI severely complicates transparency, as AI algorithms are dynamic and often inscrutable. AI presents challenges for individual due process. The development of AI technologies often excludes many affected stakeholder groups, especially underrepresented and marginalized groups. Adequate accountability for AI is often lacking. Regulatory enforcement is often overwhelmed by the tremendously high rewards for developing successful AI technologies, leading to unchecked risk taking. Remedies such as algorithmic destruction are difficult to implement in practice.

Overall, AI is not an unexpected upheaval for privacy; it is, in many ways, the future that has long been predicted. But AI starkly exposes the longstanding shortcomings, infirmities, and wrong approaches of existing privacy laws.

Ultimately, whether through patches to old laws or as part of new laws, many issues must be examined to address the privacy problems that AI is affecting. The stakes are high because AI, despite not involving sentient machines, is nevertheless an immensely powerful and transformative set of technologies. In this Article, I will provide a roadmap to the key issues the law must tackle and guidance about the approaches that will work and those that will fail.

Part I discusses what AI is and is not, dispels myths, explains why AI is both old and new, and counsels against "AI exceptionalism" – viewing AI privacy issues as so unique that they should be treated separately from other privacy issues. Part II sets forth a roadmap for the regulation of AI and privacy. I explore the privacy problems that AI raises and discuss how the law should respond.

I. AI: WHAT IS OLD IS NEW AGAIN

> Any sufficiently advanced technology is indistinguishable from magic.
>
> — Arthur C. Clarke[8]

"AI is far deeper and more powerful than just another technology," AI expert Mustafa Suleyman proclaims. "The risk isn't in overhyping it; it's rather in missing the magnitude of the coming wave. It's not just a tool or platform but a transformative meta-technology."[9]

To understand the privacy problems involved with AI and how to regulate, it is essential to understand what AI is and is not. Considerable confusion about AI currently abounds, as AI is clouded by misleading terms and metaphors.

A. THE RISE OF AI

Artificial Intelligence conjures images of intelligent robots and sci-fi fantasies. For hundreds of years, science fiction has imagined the human creation of sentient beings and machines, such as the spurned monster in Mary Shelley's *Frankenstein; or the Modern Prometheus* (1818) to Isaac Asimov's robot stories in the 1940s collected in his book, *I, Robot* (1950) to the cold and homicidal HAL in the movie, *2001: A Space Odyssey* (1968) to the friendly but annoying C3PO in *Star Wars* (1977) to the terrifying executioner robot in *The Terminator* (1984) to the synthetic human-like Data in *Star Trek: The Next Generation* (1987) to the gentle digital non-physical bot in *Her* (2013). These works captivate the public consciousness. Many people have eagerly (and sometimes with trepidation) awaited the day when AI would finally leap off the pages and screen and become reality.

But it didn't happen. Starting in the middle of the 20th Century, the digital revolution emerged with the rise of mainframe computers, then home computers, then laptop computers, then smart phones. We witnessed the rise of the Internet, the exponential growth in computing power, the vast expansion of data storage capacity, the growing power of Big Data, and the rise of the Internet of Things. But AI remained in the realm of science fiction . . . until recently.

Computer scientist John McCarthy coined the term "artificial intelligence" in 1955 at Dartmouth.[10] Many attempts were made to develop AI throughout the

[8] Quoted in Eric Siegel, *Why A.I. Is a Big Fat Lie,* Big Think, Jan. 23, 2019.

[9] MUSTAFA SULEYMAN, THE COMING WAVE: TECHNOLOGY, POWER, AND THE 21ST CENTURY'S GREATEST DILEMMA 78 (2023).

[10] CHRIS WIGGINS AND MATTHEW L. JONES, HOW DATA HAPPENED: A HISTORY FROM THE AGE OF REASON TO THE AGE OF ALGORITHMS 126-27 (2023).

ensuing decades, but these efforts typically ended in disappointment.[11] In 1973, British mathematician Sir James Lighthill famously declared in his article, *Artificial Intelligence: A General Survey*: "In no part of the field have the discoveries made so far produced the major impact that was then promised."[12] As Brian Christian puts it, the "history of artificial intelligence is famously one of cycles of alternating hope and gloom."[13]

According to technology journalist Meredith Broussard, for the first decade of this century, the mainstream public "mostly ignored AI." But then, by the middle of the 2010s, "people started talking about machine learning. Suddenly, AI was on fire again."[14] Broussard singles out 2017 as the year when AI's popularity began to rise.

The spark that ignited today's AI craze is ChatGPT, a machine learning large language model that can generate text responses to prompts. ChatGPT was developed by Open.AI, which was launched in 2015 by a group of tech leaders and investors. Originally a non-profit, Open.AI became a for-profit company in 2019. In 2021, Open.AI released ChatGPT to the public.[15]

Inspired by the success of ChatGPT, many other companies launched similar AI tools. The buzz quickly became a craze. Today, it appears AI's time has finally arrived.

B. WHAT IS AI?

The term "AI" as it is used today encompasses more than the creation of self-aware robots like those in science fiction. Instead, it involves a wide spectrum of technologies involving algorithms. An algorithm is a set of commands or instructions to perform tasks. Algorithms are akin to a mathematical recipe.

AI refers to the development of computer systems that can perform tasks typically requiring human intelligence, such as problem-solving, decision-making, language understanding, and perception. As law professor Ryan Calo notes: "There is no straightforward, consensus definition of artificial intelligence. AI is best understood as a set of techniques aimed at approximating some aspect of human or animal cognition using machines."[16]

---

[11] *Id.* at 182.

[12] WIGGINS AND JONES, HOW DATA HAPPENED, *supra* note X, at 182.

[13] BRIAN CHRISTIAN, THE ALIGNMENT PROBLEM: MACHINE LEARNING AND HUMAN VALUES 20 (2020).

[14] MEREDITH BROUSSARD, ARTIFICIAL UNINTELLIGENCE: HOW COMPUTERS MISUNDERSTAND THE WORLD 90 (2018).

[15] Rebecca Barker, "If ChatGPT Had a Brain, this Is What It Would Look Like," Fast Company (Aug. 17, 2023), https://www.fastcompany.com/90940143/if-chatgpt-had-a-brain-this-is-what-it-would-look-like.

[16] Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. Davis L. Rev. 399, 404 (2017).

1. Machine Learning, Neural Networks, and Generative AI

At the core of modern AI are machine learning algorithms. Most uses of the term "AI" today are referring to machine learning. These algorithms can simulate intelligence, but they are not actually intelligent.

Machine learning algorithms make inferences or predictions based on data. These algorithms improve and evolve with the input of increasing amounts of data, called "training data." Computer "programmers choose a machine learning model to use, supply the data, and let the computer model train itself to find patterns or make predictions." Machine learning algorithms depend upon vast quantities of data; "The more data, the better the program."[17]

One type of machine learning, called "neural networks" involve what are known as "deep learning" algorithms. Neural networks are "inspired by the human brain, mimicking the way that biological neurons signal to one another."[18] Neural networks operate through various layers, called "nodes" – designed to work as an artificial neuron. Each node is linked to others and possesses an assigned weight and threshold. A node activates and transmits data to the next layer in the network if its output surpasses this threshold. Otherwise, it remains inactive, halting the data flow.

The current public attention with AI involves generative AI, which is a branch of artificial intelligence that specializes in creating new content, whether it be text, voice, images, or video. An example of generative AI is a large language model (LLM) chatbot, such as ChatGPT. Users interact with these AI tools by inputting a "prompt" – a query or request – to which the generative AI responds by producing a response. ChatGPT is integrated with an image generating tool called DALL-E. Generative AI can produce novel and relevant outputs based on the prompts it receives.

AI and automation are often spoken about together, but they are not the same thing. AI is a form of automation, but the term "automation" more broadly encompasses "the technique of making an apparatus, a process, or a system operate automatically."[19] Many forms of automation do not involve data, and of the automated processing that involves data, many forms do not involve the types of machine learning algorithms that are now referred to as AI.

[17] Sara Brown, *Machine Learning, Explained*, MIT Sloan School of Management (Apr. 21, 2021), https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained.

[18] IBM, *What Is a Neural Network?* https://www.ibm.com/topics/neural-networks.

[19] Merriam-Webster Dictionary, *Automation,* https://www.merriam-webster.com/dictionary/automation.

2. Rebranded Old Technologies

What makes discussions of AI today so confusing is that AI is a term used to rebrand machine learning technologies. As machine learning expert Eric Siegel declares, "A.I. is a big fat lie." AI is "a hyped-up buzzword that confuses and deceives. . . . AI is nothing but a brand. A powerful brand, but an empty promise."[20] According to Siegal, a "much better, precise term [for the technologies currently labeled AI] would instead usually be *machine learning* – which is genuinely powerful."[21]

Machine learning is not new. It is actually an old technology that has been developed for about eighty years. In 1943, neurologist Warren McCulloch and logician Walter Pitts published a paper called *A Logical Calculus of Ideas Immanent in Nervous Activity*. They thought the paper would influence neuroscience, but instead it harbored the foundational ideas of neural networks.[22] The next important development was Donald Hebb's book, *The Organization of Behavior: A Neuropsychological Theory*, published in 1949.

In 1957, psychologist Frank Rosenblatt developed a machine called the "perceptron" – a gigantic computer hailed as the first neural network.[23] The machine attracted coverage in the *New York Times* and *The New Yorker,* which stated that "it strikes us as the first serious rival to the human brain ever devised."[24] But despite initial promise, the perception ultimately ended up with dashed expectations. It failed because "it had only one layer, while modern neural networks have millions."[25]

The term "machine learning" began being used in 1959.[26] But development of the technology was slow and of questionable promise. The legendary computer scientist Marvin Minsky had reservations about the viability of machine learning, publishing a book with computer scientist Seymour Papert in 1969 that cast doubt on the direction of the research at the time.[27] The book resulted in "very little research . . . in this area until about the 1980s" and "the reduction of funding for AI research in the world for more than two decades" – a period referred to as "the first winter of AI."[28]

---

[20] Eric Siegel, *Why A.I. Is a Big Fat Lie,* Big Think, Jan. 23, 2019.

[21] *Id.*

[22] CHRISTIAN, ALIGNMENT PROBLEM, *supra* note X, at 2-3.

[23] Melanie Lefkowitz *Professor's Perceptron Paved the Way for AI – 60 Years Too Soon*, Cornell Chronicle (Sept. 25, 2019), https://news.cornell.edu/stories/2019/09/professors-perceptron-paved-way-ai-60-years-too-soon.

[24] *Id.*

[25] *Id.*

[26] BROUSSARD, ARTIFICIAL UNINTELLIGENCE, *supra* note X, at 91.

[27] CHRISTIAN, ALIGNMENT PROBLEM, *supra* note X, at 20-21.

[28] Alexander L. Fradkov, *Early History of Machine Learning,* 53 ScienceDirect 1385, 1387 (202).

But machine learning continued to develop. Breakthroughs occurred during the 1990s. As machine learning expert Eric Siegel relates, he began teaching courses in machine learning in 1997, and "neural networks were already steering self-driving cars, in limited contexts."[29]

By the turn of the 21st Century, machine learning took off. The term "machine learning" was included in the Oxford English Dictionary in 2000.[30] As Alexander Fradkov notes, the first decade of the 21st Century was a "turning point" in machine learning history caused by "three synchronous trends" – the vast amount of data available, reductions in the "cost of parallel computing and memory" and the "development of the new algorithms of deep machine learning."[31]

What we have witnessed with AI is actually the rise and breakthrough of machine learning technologies. As mathematician Chris Wiggins and historian Matthew Jones contend, "Machine learning, especially machine learning using neural nets, was rebranded as AI by corporate consultants and marketers, sometimes to the discomfort of researchers."[32] When machine learning was being developed, "few thought of these efforts as 'AI.'"[33]

As law professor Ryan Calo aptly notes, "nearly every technique [of AI] we use today . . . was developed decades ago."[34] What is new, Calo argues, is that "a vast increase in computational power and access to training data has led to practical breakthroughs in machine learning, a singularly important branch of AI."[35] And now, Calo notes, "policymakers are finally paying close attention."[36]

3. Misleading Metaphors

Although AI is a misleading label for machine learning, the train has left the station, and there likely is no turning back. Now, AI has become the magic buzzword. Like the word "abracadabra," using the term "AI" opens doors, attracting investors, money, excitement, and attention. As a result, in the tech industry, the label of AI is being slapped onto nearly any piece of code. These days, it can be hard to know what really counts as AI.

AI is both a term and a metaphor. Metaphors serve as a lens through which we

---

[29] Eric Siegel, *Why A.I. Is a Big Fat Lie,* Big Think, Jan. 23, 2019.

[30] MEREDITH BROUSSARD, ARTIFICIAL UNINTELLIGENCE: HOW COMPUTERS MISUNDERSTAND THE WORLD 91 (2018).

[31] Fradkov, *Early History, supra* note X, at 1387.

[32] WIGGINS AND JONES, HOW DATA HAPPENED, *supra* note X, at 190-91.

[33] *Id.* at 140.

[34] Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. Davis L. Rev. 399, 401-02 (2017).

[35] *Id.*

[36] *Id.*

view and interpret things, offering comparisons that shape our understanding and thought processes. As Ryan Calo insightfully observes, "Every metaphor is, in its own way, an argument."[37] Metaphors have the dual capability to both clarify and skew our perception, often performing these two roles at the same time.

None of what is called AI today is actually intelligent – or even artificial.[38] AI is essentially math plus data. Even the term machine "learning" is misleading because machines don't learn as humans do. "Learning" implies a brain that gains knowledge and understanding. Machine learning algorithms essentially recognize patterns by being fed enormous quantities of data. As Meredith Broussard explains, machine learning "means that the machine can improve at its programmed, routine, automated tasks" not that "the machine acquires knowledge or wisdom or agency, despite what the term *learning* might imply."[39]

Ultimately, the promise of sentient robots still has yet to be realized. But today, we hear the grand proclamations that AI is here. Instead, a set of related technologies has finally started to work well and has been rebranded as AI.

Metaphors may give technology human-like qualities, but they can also strip it of its human essence. Our gadgets are merely assemblies of metal, plastic, and glass, and data seems to float in a detached, virtual space. Yet, the human element is always integral to technology. As noted by Kate Crawford, human involvement is deeply embedded in AI at almost every stage.[40] The data used to train AI algorithms originates from human activities, thoughts, and conversations, and it is often curated by humans too. Humans are instrumental in designing and training algorithmic models.[41] As Eric Siegel notes, the most effective machine learning is "supervised machine learning" which involves training data that is labeled. The algorithm "learns" from the labels and can confirm it is getting something right or wrong. It is humans who label this data. AI, while seemingly ethereal, is profoundly physical, rooted in intense human labor—often arduous and taxing—and reliant on substantial energy and material resources.[42]

Indeed, the AI of today might invoke a rough analogy to the Mechanical Turk, a chess-playing machine that captivated European audiences since its invention

---

[37] Ryan Calo, *Robots as Legal Metaphors,* 30 Harv. J. L. & Tech. 209, 211 (2016).

[38] Evgeny Morozov, *The Problem with Artificial Intelligence? It's Neither Artificial Nor Intelligent,* The Guardian (Mar. 30, 2023).

[39] MEREDITH BROUSSARD, ARTIFICIAL UNINTELLIGENCE: HOW COMPUTERS MISUNDERSTAND THE WORLD 89 (2018).

[40] KATE CRAWFORD, ATLAS OF AI: POWER, POLITICS, AND THE PLANETARY COSTS OF ARTIFICIAL INTELLIGENCE (2021); Rebecca Crootof, Margot E. Kaminski & W. Nicholson Price II, *Humans in the Loop*, 76 Vand. L. Rev. 429 (2023).

[41] Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. Cal. L. Rev. 1529, 1538-39 (2019).

[42] CRAWFORD, ATLAS OF AI, *supra* note X, at 53-87; IVANA BARTOLETTI, AN ARTIFICIAL REVOLUTION: ON POWER, POLITICS, AND AI 81-93 (2020).

in 1770 and for nearly eight decades thereafter. This device, with a wooden cabinet and a chessboard on top, featured an automated Turk figure seated at one end. However, it was eventually revealed to be a hoax – a human was concealed inside all along.[43] The AI of today is similarly far from artificial –it is deeply intertwined with human effort.

Using metaphors drawn from familiar concepts to comprehend new and unfamiliar ones is natural and often unavoidable. While we cannot completely avoid employing metaphors, it's crucial to be aware of the ones we choose and the potential distortions they may introduce in our understanding.

The metaphors used for AI significantly influence the shaping of laws and policy. To understand the privacy problems involved with AI, it is essential to understand how AI actually works. It matters how much data is gathered for AI, how the data is gathered, and how the data is shaped and standardized. It matters how AI tools produce their outputs, the limits of the AI's ability to produce outputs, the potential errors and skewing that can occur, and what is lost or altered in the process, as AI does not precisely simulate reality but alters it. It matters how AI tools are used. It matters how AI tools are designed – the humans behind the scenes – their motivations, goals, biases, and assumptions.

The perceptions of the users of AI matter, as well as how they rely on AI's output. Ironically, the way AI is understood distorts in ways that both anthropomorphize it by attributing it with human-like qualities as well as conceal its human dimensions. Distortion in either direction can lead us astray in how we use and regulate AI.

How we understand AI affects how much we trust it, whether we treat it as neutral or biased, how we interact with it, how we use it for decisions and other purposes, whether we recognize certain problems, and who we hold responsible for them. Ultimately, the law's response depends significantly on our understanding of AI.

C. AGAINST AI EXCEPTIONALISM

For privacy issues, we must be careful to avoid what I call "AI exceptionalism" – treating AI as so different and special that we fail to see how the privacy problems with AI are the same as existing privacy problems, just enhanced. AI represents a future for privacy that has been anticipated for a long time. AI starkly highlights the deep-rooted flaws and inadequacies in current privacy laws, bringing these issues to the forefront.

AI is starting to spook policymakers. New laws are being proposed. Although I

[43] Ifeoma Ajunwa, *The Paradox of Automation as Anti-Bias Intervention*, 40 Cardozo L. Rev. 1671, 1704-07 (2020).

certainly embrace this opportunity for legal reform, I do not take a position on whether new laws should be enacted or old laws should be changed. What matters is whether policymakers have an adequate vision of the full landscape of privacy problems with AI and a proper understanding of the problems and how to address each of them.

Some commentators are calling for special AI laws and special agencies to address AI.[44] Additional laws can be helpful, but there are some caveats. First, a general AI law risks failing to focus sufficiently on AI's privacy problems, leaving many unaddressed. AI presents an opportunity to revisit and rethink existing privacy law, which can play an essential role. Policymakers should not assume that privacy law has a handle on AI's privacy problems and that all that is needed is an additional layer of protections. Making this mistake would be akin to adding a story to a building with an unstable and poorly designed foundation.

AI's privacy problems involve practices long addressed by privacy law – the gathering and processing of personal data. To confront the privacy problems with AI, these practices must be addressed holistically and together, not just when some magical line is crossed into the realm of AI, as if it were a parallel universe. AI is continuous with the data collection and use that has been going on throughout the digital age.

In the early days of the commercial internet, Judge Frank Easterbrook famously argued that the internet should not be regulated by a separate body of law just as we don't have a separate "Law of the Horse."[45] He is partially right in that we should avoid rushing to advance new specialized laws to technologies like the internet that will affect nearly every facet of life and every area of law. AI is likely to be such a technology – it will affect an enormous array of issues and involve countless domains of law.[46] But this doesn't mean that AI lacks dimensions and issues that require special consideration.

For privacy, regardless of whether existing laws are used or new laws or a combination, we have reached a moment of reckoning. As I will explain in the rest of this Article, existing laws are not up to the task. Hopefully, policymakers will now recognize the urgent need for a fundamental shift in the approach privacy law should take.

---

[44] Andrew Tutt, *An FDA for Algorithms*, 69 Admin. L. Rev. 83 (2017).

[45] Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. Chi. Legal F. 207.

[46] Alicia Solow-Niederman, *Administering Artificial Intelligence,* 93 S. Cal. L. Rev. 633 (2020) (arguing that it will be a challenge with having a single agency regulating AI "given the dynamic and cross-cutting nature of AI").

II. A REGULATORY ROADMAP TO AI AND PRIVACY

Let us tread with care,
As we delve into AI's abyss,
And ensure we're always aware,
Of the dangers we might miss.

– ChatGPT

In this Part, I provide a regulatory roadmap to AI and privacy, and I discuss how privacy law must change and adapt to address the privacy problems of AI. The goal of this roadmap is to raise issues the law must grapple with, point out why the law's prior wrong approaches are especially deficient for AI, and propose new directions the law should take. I am not proposing a model law; instead, this is broader and more conceptual – a roadmap and a guide.

AI demonstrates why certain long overdue changes to privacy law are needed. AI is, after all, not a radically new set of technologies from those that began to raise privacy concerns in the second half of the 20th century. The difference today is more data, more computing power, and better analytics.

Many of AI's privacy problems preexisted AI and can't be solved by exclusively focusing on AI. The best way to deal with them is to focus on their roots. Trimming off the top branches will not really address the crux of these problems. AI's privacy problems are a remix of existing privacy problems, which are combined in new ways or amplified to a new degree. AI also challenges distinctions and structures in existing privacy laws; it exposes the cracks, gaps, and flaws of these laws in stark ways that demand attention.

This Part begins with a broad analysis of the architecture and approaches of privacy regulation – the foundations of these laws, which have long been unsuitable to address privacy problems in the digital age. AI threatens to collapse the entire edifice. There is no easy retrofit; the foundation must be rebuilt.

Next, I turn to how privacy law should regulate data collection. AI's insatiable appetite for data severely challenges privacy law's regulation of data collection. Inconsistent concepts and approaches in privacy law are inadequate to address scraping, the process by which much data for AI is gathered. Legal approaches to consensual data gathering must also be revisited.

The focus then turns to data generation. AI enables extraordinary abilities to generate data, which exacerbates many privacy problems. AI creates inferences, which involve new data being created about individuals that they don't expect

and never wanted to share. Inference blurs the line between data processing and collection, which allows it to evade data collection limitations and other protections in many privacy laws. AI can also generate malevolent material – deceptive and manipulative content that can cause severe harm to people and society. AI's ability to simulate humans and human-made content can open up new dimensions in deception and manipulation.

AI also impacts privacy through its use in decision-making about people. AI alters the way decisions are made, facilitating predictions about the future that can affect people's treatment and opportunities. These predictions raise concerns about human agency and fairness. AI is also used in non-predictive decisions about people, transforming the way bias affects these decisions. As AI decision-making involves automation, there are problems caused by automated processes that the law has thus far struggled to address.

AI also enables unprecedented data analysis, which can greatly enhance surveillance and identification. Privacy law has long inadequately addressed the problems caused by surveillance and identification. AI threatens to take these problems to new heights and add troublesome new dimensions.

Lastly, this Part addresses how privacy laws should handle oversight, participation, and accountability for AI. The way AI technologies work complicates traditional oversight mechanisms, such as transparency, as AI operates in large part as a black box. AI presents due process challenges, making it difficult for individuals to challenge its decisions and effects. The development of AI tools often excludes the participation of many stakeholders, making it unrepresentative and lacking in diversity. Accountability for AI also must be improved, as well as effective remedies for privacy violations.

A. LEGAL ARCHITECTURE AND APPROACHES

1. Beyond Individual Control and Self-Management

Privacy law has been dominated by a model of individual control, which endeavors to empower individuals by allowing them to manage their own personal information, a set of tasks I term collectively as "privacy self-management."[47]

In the U.S., many privacy laws aim to facilitate individual control through the "notice-and-choice approach."[48] Organizations post notices about the data they collect, how they use and transfer it, and how they protect it. People can opt out or stop doing business with companies. If people don't opt out, they are assumed

[47] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 Harv. L. Rev. 1880, 1880 (2013).

[48] *See id.* at 1883-84; Charlotte A. Tschider, *Meaningful Choice: A History of Consent and Alternatives to the Consent Myth,* 22 N.C. J.L. & Tech. 617 (2021).

to have consented. Many U.S. privacy laws mandate that companies provide opt out rights to particular uses.[49] Some laws require that people expressly consent (opt in) for certain uses.[50] As professor Daniel Susser characterizes the notice-and-choice approach, "businesses can do what they want with user information provided (1) they tell users that they are going to do it and (2) users choose to proceed."[51]

For decades, the notice-and-choice approach has long been attacked by countless experts for being ineffective, and for some, downright farcical.[52] As described by law professors Woodrow Hartzog and Neil Richards, "'Notice' often means little more than burying data practices in the fine print of a dense privacy policy, while 'choice' means choosing to use a service with its non-negotiable data practices as a take-it-or-leave-it option."[53] The problem is that hardly anyone reads privacy notices; if people try to read them, they struggle to understand them; reading each company's privacy notice would take an unreasonable amount of time; and it is not clear that such notices help people make informed risk decisions about the collection and use of their data.[54]

In the EU, the GDPR also has a strong core of individual control. In contrast to the notice-and-choice approach in the U.S., the GDPR rejects opt out consent. Consent must be express, which means that people must opt in.[55] The GDPR buttresses individual control by providing individuals with many rights, such as rights to access, rectify, or erase their data, as well as rights to data portability, to object to certain instances of data processing, and to challenge automated decision-making.[56] The GDPR also imposes several duties on organizations, such as requirements to conduct data protection impact assessments, engage in data minimization, maintain records of processing activities, and ensure data protection by design and default.[57] But as law professor Ari Waldman notes, these duties are often carried out internally at companies in a hollow "symbolic"

---

[49] *See, e.g.,* CAN-SPAM Act, 15 U.S.C. § 7704(a)(3) (provides right to opt out of receiving unsolicited commercial emails); Telephone Consumer Protection Act, 47 U.S.C. § 227 (provides right to opt out of telemarketing calls).

[50] *See, e.g.,* Children's Online Privacy Protection Act, 15 U.S.C. § 6502(b) (parents must opt in to the collection and use of their children's data); Video Privacy Protection Act, 18 U.S.C. § 2710(b)(2)(B) (opt in for disclosure of consumer personal data).

[51] Daniel Susser, *Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't,* J. Info. Policy 37, 41-42 (2019).

[52] Neil Richards and Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Wash. U. L. Rev. 1461, 1463 (2019); Richard Warner & Robert Sloan, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. High Tech. L. 370 (2014); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 Daedalus 32, 34 (2011).

[53] Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection,* 61 B.C. L. Rev. 1687, 1704 (2020)

[54] Solove, *Murky Consent, supra* note X, at X.

[55] GDPR art. 4.11 (requiring "clear affirmative action" for valid consent).

[56] *See* GDPR Chapter III, *Rights of the Data Subject,* art. 12-23.

[57] GDPR art. 35 (data protection impact assessments); art. 30 (records of processing activities); art.25 (data protection by design and by default); art. 5(c) (data minimization).

way.[58] Many duties exist largely to minister to individual rights. Although the GDPR laudably advances beyond individual control, the regulation still places far too much weight on it.

Partly due to the influence of the GDPR, U.S. privacy law has supplemented the rather barebones notice-and-choice approach with rights such as the right to access, correct, and delete, as well as the right to data portability.[59] Several states provide rights to opt out of automated data processing under certain circumstances.[60]

The control afforded by privacy law places the onus on individuals to manage their own privacy, something they are ill-equipped to do.[61] Although express consent is far superior to the notice-and-choice approach, it still depends heavily on the ability of individuals to make meaningful decisions about the collection and use of their data. Privacy laws are, in essence, delegating to individuals the responsibility to manage their own privacy, which can be more of a burden than a benefit.[62] The onus is on individuals to exercise their privacy rights, which is a difficult if not impossible to do with the thousands of companies that collect and use their data. People don't have time to manage their data with each one.[63]

Moreover, people lack the expertise to determine whether the collection, use, or disclosure of their personal data will create a risk of harm. In today's world of AI, the algorithms that power automated decisions are far too complex for people to understand. These algorithms depend on enormous quantities of data; to be able to assess their risks, people must become expert data scientists and also be able to review the data used to train the algorithms, which isn't feasible.[64]

Rather than truly empowering individuals, the law creates a façade of empowerment, ironically leading to further disempowerment. This situation saddles people with endless unachievable tasks; when people predictably don't do all this work, they are blamed for not caring about their privacy.[65]

AI algorithms work with large collective datasets, not with isolated individual data. In the modern "inference economy," as Alicia Solow-Niederman terms it,

---

[58] ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 115 (2021).

[59] *See* Va. Code Ann. § 59.1-575 (2023); Colo. Rev. Stat. § 6-1-1303(24) (2021); Utah Code Ann. § 13-61-101(32) (2023); 2023 Conn. Pub. Acts No. 22-15 § 1(27).

[60] Liisa M. Thomas, *The Comprehensive Privacy Law Deluge: What to Do About "Profiling,"* National L. Rev. (June 26, 2023).

[61] Daniel J. Solove, *The Limitations of Privacy Rights,* 98 Notre Dame L. Rev. 975, 993 (2023).

[62] Ella Corren, *The Consent Burden in Consumer and Digital Markets,* 36 Harv. J. L. & Tech. 551 (2023).

[63] *See* Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies,* 4 I/S 540, 565 (2008) (reading all privacy notices would take more than 200 hours a year).

[64] Solove, *Murky Consent, supra* note X, at 127-29.

[65] Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 Geo. Wash. L. Rev. 1, 11-14 (2021).

which is driven by machine learning and algorithmic decision-making, the role of data is fundamentally collective.[66] These technologies operate by drawing inferences from datasets that include information about many people. As Salomé Viljoen points out, algorithms identify similarities among individuals, uncovering meaningful insights about our biological, interpersonal, political, and economic connections.[67] Solow-Niederman and Viljoen emphasize the relational nature of data.

AI algorithms typically involve identifying patterns within large datasets that encompass millions of individuals. Within this context, rights and protections that focus solely on the individual fall short. Individuals trying to understand how decisions are made or how their personal data is used within these systems can only grasp a fraction of the picture. To fully comprehend the decision-making processes of these algorithms, it is necessary to consider the collective data of all individuals included in the algorithm's dataset. But this data can't be provided to individuals without violating the privacy of the people in the dataset; nor is it feasible for individuals to analyze this enormous magnitude of data.

Privacy rights often fall short because they typically concentrate on individual-level concerns, such as the accuracy of a person's records or whether they consented to their data being collected. However, these approaches are inadequate for tackling systemic problems. For instance, while the Fair Credit Reporting Act (FCRA) allows individuals to correct errors in their records, it doesn't challenge the foundational principles of credit scoring systems.[68] Individuals may have the ability to rectify mistakes in their data, but they lack any influence or recourse over the methodologies used to judge their creditworthiness. As long as consumer reporting agencies provide access and rectification options, they retain considerable latitude in their decision-making processes. This overlooks the potential unfairness and issues stemming from the algorithms these companies use.[69]

The rise of AI has made it emphatically clear that the individual control model is doomed. AI is far too vast and complicated for individuals to understand and to assess the impact on their privacy. Instead of trying to provide individuals with control over their data, the law should bring the collection and use of data under control. Although in some circumstances, privacy rights can be helpful, privacy laws should stop relying on them so heavily and focus more on structural measures that don't place the burden on individuals. Effective privacy protection must focus on the architecture of the modern digital economy; it must impose meaningful duties on organization to avoid risks and harms; and it must hold

[66] Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 Nw. L. Rev. 357, 361 (2022).

[67] Salomé Viljoen, *Democratic Data: A Relational Theory for Data Governance*, 131 Yale L.J. 573, 578-79 (2021).

[68] Fair Credit Reporting Act, 15 U.S. Code §1681. FCRA requires "reasonable procedures to assure maximum possible accuracy" §1681e(b) and allows individuals to dispute accuracy. §1681i(a)(1).

[69] Solove, *Limitations of Privacy Rights, supra* note X, at 1034.

organizations accountable in meaningful ways.[70]

2. Harm and Risk Analysis

New laws addressing AI are taking a different approach. Instead of focusing on individual control, these laws look to harms and risks. Leading the charge is the EU with its AI Act.[71] The Act creates three categories of risk: (1) an unacceptable risk, (2) a high risk, and (3) limited risk. AI systems creating an unacceptable risk are banned. For the other two risk categories, restrictions and protections are proportionate to the category. As law professor Margot Kaminski points out, the "central concept behind risk regulation is that in the face of uncertainty, regulators should not ban or overregulate technologies, but rather aim their efforts at lessening known and measurable harms."[72]

Focusing on harms and risks is a step in the right direction, something privacy law as a whole should do, not just for AI.[73] To a limited extent, some privacy laws focus on harm and risk. For example, many privacy laws require risk assessments under certain circumstances. The GDPR has a requirement that organizations must conduct a data protection impact assessment (DPIA) in situations involving a "high risk to the rights and freedoms of natural persons."[74] The "rights and freedoms" include both privacy and fundamental rights, such as "freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion."[75] The GDPR lists three examples of high risk processing, one of which includes the "systemic and extensive processing activities, including profiling, where decisions have legal effects or similarly significant effects on individuals."[76] Inspired by the GDPR, many U.S. state consumer privacy laws require risk assessments for automated decision-making or profiling.[77]

But there are still challenges to the harm and risk approach that the law must grapple with. Margot Kaminski raises the concern that risk regulation

---

[70] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 101 (2004) ("[T]he protection of privacy depends upon an architecture that structures power, a regulatory framework that governs how information is disseminated, collected, and networked. We need to focus on controlling power."); Dennis Hirsch, *New Paradigms for Privacy Law,* 79 Md. L. Rev. 439, 462 (2019) (new proposals for privacy emphasize "social protection, rather than individual control [in a] shift from a liberalist regulatory approach that seeks to facilitate individual choice, to one that empowers public officials to make choices about which . . . practices are safe for individuals and consistent with social values, and which are not.").

[71] European Commission, *Artificial Intelligence – Questions and Answers* (Dec. 12, 2023), https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683.

[72] Margot E. Kaminski, *Regulating the Risks of AI*, 103 B.U. L. Rev. 1347 (2023).

[73] Daniel J. Solove, *Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data*, 118 Nw. U. L. Rev. 1081, 1128-36 (2024).

[74] GDPR art. 5.

[75] GDPR art. 5.

[76] GDPR art. 5.

[77] Liisa M. Thomas, *The Comprehensive Privacy Law Deluge: What to Do About "Profiling,"* National L. Rev. (June 26, 2023).

frameworks are often "not well suited to unquantifiable and contested individualized harms."[78] Although the individual control model is insufficient to address AI's privacy problems, AI still harms individuals, and these harms should be redressable. Relying less on individual control doesn't entail failing to safeguard against harm. A harm and risk approach must address harms and risks to both society and individuals and must provide mechanisms of redress to harmed individuals.

A vexing issue with the harm and risk approach is determining who should assess the harms and risks. Should organizations be responsible for assessing the harms and risks of their own AI systems? Or should a government agency do the assessing? Most laws rely on organizations to assess the risks they create, which can be akin to asking the fox to assess the danger to the chickens in the henhouse.

When organizations are the ones doing the assessment, a challenging issue is whether the law should require that the assessments be shared with regulators or the public. Most laws lack such a requirement.[79] Disclosing assessments outside the organization would make organizations more accountable, preventing them from doing cursory assessments and then taking no action in response. On the other hand, requiring the sharing of risk assessments might reduce their candor and turn them more into an external public relations exercise.

Another difficult issue is how to handle generative AI or other AI tools that are used in myriads of different ways by users. With so many uses, there could be many potential harms and risks. Natali Helberger and Nicholas Diakopoulos contend that a risk analysis of generative AI will be challenging because "Generative AI systems are not built for a specific context or conditions of use, and their openness and ease of control allow for unprecedented scale of use."[80] As Josephine Wolff, William Lehr, and Christopher Yoo argue, "the central problem posed by general purpose AI is that it is nearly impossible to assess the risks associated with it in any meaningful way."[81] Further, they argue that for the "GDPR, the key problem is that it is nearly impossible to perform any meaningful purpose limitation (or data minimization) for data used to train general AI systems."[82]

Yet another issue is the timing of regulatory review. Should regulators review AI technologies before they are deployed? Doing so could come perilously close to

[78] Kaminski, *Risks of AI, supra* note X, at 1379.

[79] A notable exception includes the CCPA, §1798.185(a)(15), which requires risk assessments to be submitted to regulators.

[80] Natali Helberger & Nicholas Diakopoulos, *ChatGPT and the AI Act,* 12 Internet Pol'y Rev. 1, 3 (2023).

[81] Josephine Wolff, William Lehr, and Christopher Yoo, *Lessons from GDPR for AI Policymaking,* 27 Va. J. L. & Tech. 1, 22 (2024).

[82] *Id.*

turning into a licensing system, which can slow innovation with waiting periods while regulators conduct a review. Review of AI after deployment might come too late to stop their harms. These issues will ultimately need to be examined and balanced in harm and risk approaches.

B. DATA COLLECTION

AI has ushered in an unprecedented amount of data collection.[83] Personal data for AI is gathered primarily in two ways – through scraping the data from the internet or by repurposing customer or user data. AI's thirst for data is placing tremendous stress on privacy laws, which attempt to place meaningful controls on data gathering. In many instances. AI could evade the protection of many privacy laws. In other circumstances, some laws, if strictly interpreted and enforced, would greatly restrict the collection of data for AI, starving it of the data needed to function. Finding a middle ground between a data feeding frenzy or data famine will be difficult.

1. Scraping

Machine learning algorithms require extensive data for training, and the internet is the most accessible feeding ground. For example, a company called Clearview AI developed one of the leading facial recognition tools by harvesting billions of photos it scraped from social media, online profiles, and photography websites. The company did this without seeking consent, using images that individuals never anticipated would be part of a vast AI network for law enforcement and government surveillance.[84] Many entities are engaging in similar data scraping practices. Various organizations relentlessly extract online data to feed the insatiable needs of their AI systems.[85]

(a) Scraping and Privacy Principles

Web scraping contravenes many commonly recognized privacy principles in laws, industry codes, or accepted standards. These principles include being transparent about personal data collection and usage; informing individuals about their privacy policies; define the objectives for using personal data; preventing data use for unrelated secondary purposes; seeking consent for data use or offer opt-out options; providing information about third-party data

[83] Charlotte A. Tschider, AI's Legitimate Interest: Towards a Public Benefit Privacy Model 21 Hous. J. Health L. & Policy 125, 132 (2021) ("Machine learning applications use exceptionally large volumes of data, which are analyzed by a machine learning utility to determine interrelationships between these data.").

[84] KASHMIR HILL, YOUR FACE BELONGS TO US; A SECRETIVE STARTUP'S QUEST TO END PRIVACY AS WE KNOW IT (2023).

[85] Kieran McCarthy, "Web Scraping for Me, But Not for Thee," Tech. & Marketing L. Blog (Aug. 24, 2023) (nothing that ChatGPT has "almost certainly already scraped the entire non-authwalled-Internet" and used the data to train ChatGPT), https://blog.ericgoldman.org/archives/2023/08/web-scraping-for-me-but-not-for-thee-guest-blog-post.htm.

recipients; performing due diligence prior to data transfer to third parties; establishing agreements with third-party recipients of personal data to ensure data protection; granting individuals rights over their personal data, including access, correction, deletion, and portability; retaining data only as long as necessary for the stated purposes; disposing of data appropriately; maintaining data accuracy; and safeguarding against unauthorized data access.[86] Scraping essentially ignores all of these principles; data is just taken by third party scrapers without any notice, consent, vetting, safeguards, specified purposes, purpose limitations, data minimization, individual rights, retention limitations, and more. Essentially, scraping is bereft of any privacy considerations.

Scraping occurred long before machine learning algorithms became popular and entered widespread use. Scraping thus isn't a problem exclusive to AI. But AI dramatically escalates scraping because AI creates incentives to scrape more frequently and extensively.

(b) Publicly Available Data

In the U.S., scraping has so far avoided significant engagement with privacy laws, largely because it targets data that seems publicly accessible online. Those who scrape often operate under the assumption that no privacy concerns apply to such publicly available data, believing it to be freely accessible.

Many privacy laws adopt a simplistic binary concept of privacy, viewing personal data as private only if it is concealed – a concept I term the "secrecy paradigm."[87] Privacy, however, is far more complex; it entails a series of boundaries that module how data is shared.[88] Individuals rarely keep their data entirely private. More commonly, they disclose it within specific social confines, such as to friends, family, work colleagues, or members of groups with shared interests, like those facing similar health challenges or battling the same addictions.

As several scholars have persuasively argued, people expect some degree of privacy in public, and such expectation is reasonable as well as important for freedom, democracy, and individual well-being.[89] In everyday life, much of our

[86] Although only some privacy laws include all of these principles, such as the GDPR and CCPA, many privacy laws include most of these principles. Additionally, many of these principles are found in influential frameworks such as the Organization for Economic Co-operation and Development (OECD) Guidelines of 1980; the National Institute of Standards and Technology (NIST) *Privacy Framework* (Jan. 6. 2020), https://www.nist.gov/privacy-framework; and the AMERICAN LAW INSTITUTE'S PRINCIPLES OF THE LAW, DATA PRIVACY (May 22, 2019).

[87] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004).

[88] Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 University of Chicago Law Review 919 (2005).

[89] Helen Nissenbaum, *Protecting Privacy in the Information Age: The Problem of Privacy in Public*, 17 Law & Phil. 559 (1998); Helen Nissenbaum, *Toward an Approach to Privacy in Public: Challenges of Information Technology*, 7 Ethics & Behav. 207, 208 (1997); Joel R. Reidenberg, *Privacy in Public*, 69 U. Miami L. Rev. 141, 157-59 (2014); Woodrow Hartzog, *The Public Information Fallacy,* 99 B.U. L. Rev. 459, 522 (2019).

data is protected by practical obscurity.[90] Even though data might be exposed to the public, there still can be a privacy interest in the data because it is hard to find, not normally observed or recorded, and fragmented and widely dispersed. Moreover, as intellectual property law demonstrates, it is possible for the law to provide robust protections to information even if publicly available.[91] Privacy law also does this in some circumstances, such as the tort of appropriation of name or likeness which provides protection despite the public availability of this data.[92]

For privacy protection to be truly effective in the age of AI, the law must move beyond simplistic binary perspectives and start safeguarding obscurity.[93] Organizations should not be able to indiscriminately collect personal data from the internet for any purpose they see fit.

Privacy law's stance on publicly available data is currently inconsistent. While some laws, like those in the EU's General Data Protection Regulation, do not exempt publicly available data in most circumstances, other laws do.[94] For example, the California Consumer Privacy Act (CCPA) exempts "publicly available information" which includes data from government records as well as data published in widely-distributed media or made available to the general public by the data subject or another person where the data subject has not restricted the data to a specific audience.[95] Other states, such as Utah and Virginia, have similar exemptions in their consumer privacy statutes.[96] But some states, although exempting "publicly available information," have a much narrower definition of the term. For example, Colorado only includes data in government records and data that the data subject has made available to the general public.[97] Connecticut includes the same categories as Colorado but also data disseminated by the media.[98] For example, as privacy lawyer David Zetoony observes, "while some businesses may consider information that is available on the internet to be 'publicly available information,' most data privacy statutes would not classify all internet-accessible information as being 'publicly available.'"[99]

---

[90] Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 Wash. & Lee L. Rev. 1343, 1349 (2015).

[91] DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 184-86 (2007).

[92] Restatement (Second) of Torts §652C.

[93] Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 Wash. L. Rev. 385, 407 (2013). I have discussed the problem of obscurity by using the term "increased accessibility." SOLOVE, UNDERSTANDING PRIVACY, supra, at

[94] The GDPR generally protects against publicly available data, but it exempts "personal data which are manifestly made public by the data subject." GDPR art. 9.2(e).

[95] Cal. Civ. Code § 1798.140(v)(2) (West 2021).

[96] Va. Code § 59.1-571 (2021); Utah Code Ann. § 13-61-101(29)(b) (2022).

[97] C.R.S. § 6-1-1303(17)(b) (2021).

[98] Connecticut Data Privacy Act, § 1(25).

[99] David Zetoony, *What is 'Publicly Available Information' under the State Privacy Laws?* National Law Review (Sept. 13, 2023) https://www.natlawreview.com/article/what-publicly-

Some U.S. federal laws do not exclude publicly available data. For example, the Fair Credit Reporting Act (FCRA), which regulates credit reporting, protects all data that consumer reporting agencies gather and use, no matter whether the source was public or private. Much of the data used in credit reporting is obtained from public records, such as data about property, licenses, criminal convictions, civil judgments, bankruptcies, and more. HIPAA protects health data even if it is publicly available.[100]

In many cases, personal data on platforms is not free for the taking but limited in use by the platform's terms of service. These terms of service are not mere suggestions; they are *terms*. LinkedIn has a user agreement which requires users to not use software, bots, or processes to scrape user profiles.[101]

Moreover, legal precedents, such as in the U.S. Supreme Court cases *Carpenter v. United States* and *DOJ v. Reporters Committee for Freedom of the Press*, have acknowledged that public availability does not negate an individual's privacy rights. In *Carpenter*, the Court ruled that collecting geolocation data of public vehicle movement breached reasonable privacy expectations. The Court's decision marked a significant shift in its approach to privacy. Previously, the Court had maintained that anything observable in a public place was not private.[102] However, in *Carpenter*, the Court acknowledged that geolocation data, despite often tracking movement in public areas, opens up an "intimate window into a person's life."[103] The Court determined that there is a reasonable expectation of privacy in GPS data, warranting Fourth Amendment protection and necessitating that law enforcement obtain a search warrant to access such data.

In *Reporters Committee*, the Court recognized that personal data in public records still retains a privacy interest. A media organization sought access to FBI dossiers on individuals, claiming they were public information under the Freedom of Information Act, which contains a privacy exemption. The media argued that the information wasn't private as it was sourced from various public records. However, the Court disagreed, stating, "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[104]

available-information-under-state-privacy-laws.

[100] HIPAA contains no exemption if the health data it protects is publicly available.

[101] LinkedIn, User Agreement 8.2, https://www.linkedin.com/legal/user-agreement.

[102] United States v. Knotts, 460 U.S. 276 (1983) (no reasonable expectation of privacy when tracking device monitored movement in public); Florida v. Riley, 488 U.S. 445 (1989) (no expectation of privacy in anything that can be viewed on one's property by police officers in a helicopter flying in legal airspace).

[103] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[104] U.S. Dep't of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).

Thus, U.S. privacy law is inconsistent about whether public exposure or public accessibility means that there no longer is a privacy interest in data. For privacy protection to be effective, legal frameworks need to move beyond binary definitions and safeguard obscurity.

A related issue involves the obligations that platforms and other organizations have to protect data against being scraped. Privacy laws generally do not mandate that a site protect against scraping. It is up to organizations to protect user data in their terms of service and then to enforce their terms of service. But privacy laws should mandate protection against scraping. If an organization attempted to transfer massive amounts of personal data to third parties without consent, this practice would violate many privacy laws. Failing to prevent third parties from just taking the data is the functional equivalent of selling or sharing it.

(c) Responsible Public Records

Given the problems emerging from the indiscriminate collection and use of personal data for AI systems from records online, it is essential for the government to finally exercise responsible control over the personal data it routinely disseminates to the public.

Originally, open records laws were enacted to increase transparency in government operations. Nowadays, however, public records are predominantly utilized by Big Data companies for collecting and assembling personal data. Laws intended to empower people to shed light on their government are instead shedding light on people.[105] Public records should not be a free unlimited fountain of data for AI.

In the case of *Los Angeles Police Department v. United Reporting Publishing Co.*, a statute limited access to public arrestee information, requiring declarants to affirm under penalty of perjury that the data would not be used "directly or indirectly to sell a product or service." This statue was challenged on the grounds of infringing commercial speech. The U.S. Supreme Court, however, did not view the statute as a speech restriction. Rather, the statute is not "prohibiting a speaker from conveying information that the speaker already possesses" but is merely "a governmental denial of access to information in its possession."[106]

The implication is that the government can place conditions on much of the data it releases to the public, similar to how a company can provide conditions in its terms of service. Governments can make public records available on the condition that certain information is not used in certain ways. This distinction strikes a practical balance. Conditional access allows the public to access a broad

[105] Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 Minn. L. Rev. 1137, 1176-78 (2002).
[106] 528 U.S. 32 (1999).

array of records while simultaneously protecting privacy.

Beyond being allowable under the First Amendment, conditions on the access to personal data in public records should be an obligation of the government under the law. The law should require government entities to place reasonable conditions on access to personal data. By dumping personal data on the internet without any protection, government agencies are acting irresponsibly.

2. "Consensual" Data Collection

(a) Fictions of Consent

Companies have started to change their privacy notices to indicate they will use people's data for the development of AI. For example, in 2023, Zoom changed its privacy notice to state that users were consenting to Zoom's "access, use, collection, creation, modification, distribution, processing, sharing, maintenance, and storage of Service Generated Data for any purpose." The notice stated that "any purpose" included the training of AI algorithms. Zoom also included a clause where the user granted to Zoom "a perpetual, worldwide, non-exclusive, royalty-free" license to use their content for AI training and any other purpose. However, Zoom's change caught public attention, and the company backtracked.[107]

In the same year, Google and other companies changed their privacy notices to provide for AI collection. Google stated that "we use publicly available information to help train Google's AI models and build products and features like Google Translate, Bard, and Cloud AI capabilities."[108] X, formerly Twitter, changed its privacy notice to state: "We may use the information we collect and publicly available information to help train our machine learning or artificial intelligence models for the purposes outlined in this policy."[109]

The practice of changing privacy notices and collecting and using personal data for new purposes is a common one, not just limited to AI. In many U.S. privacy laws, such a practice is commonly permitted under the notice-and-choice approach.[110]

Although the EU's GDPR rejects the notice-and-choice approach and instead

[107] Ian Krietzberg, "Zoom Walks Back Controversial Privacy Policy," The Street (Aug. 11, 2023).

[108] Matthew G. Southern, "Google Updates Privacy Policy to Collect Public Data For AI Training," Search Engine Journal (July 3, 2023), https://www.searchenginejournal.com/ google-updates-privacy-policy-to-collect-public-data-for-ai-training/490715/.

[109] Sarah Perez, "X's Privacy Policy Confirms It Will Use Public Data to Train AI Models," Tech Crunch (Sept. 1, 2023).

[110] Examples of U.S. privacy law's notice-and-choice approach include the CAN-SPAM Act, 15 U.S.C. §7704(a)(3) (allowing companies to send send unsolicited commercial emails to people unless people opt out)l Telephone Consumer Protection Act, 47 U.S.C. §227 (allowing telemarketers to call people unless people opt out).

requires express consent (opt in),[111] even this stronger form of consent is not meaningful. Often, such consent merely requires clicking an accept button; it doesn't guarantee that people have read the privacy notice or understand the risks involved. Even forcing people to indicate express consent through an agree button or box leads to hardly any increase in the readership of a notice.[112] In other work, I've argued that no matter whether consent is opt out or opt in, it is still largely a fiction.[113]

AI further complicates the equation; it makes the fiction more fanciful. With generative AI, for example, the specific uses are often unknown; users of generative AI tools can use them for a myriad of different uses, some benign, some malignant. Consent becomes a blank check to do nearly anything. With AI, people often have no idea what they are consenting to.

AI amplifies the shortcomings of approaches to consent, but privacy law has long been flawed by relying too heavily on consent. Whether opt in or opt out, whether under U.S. privacy laws or the GDPR or many privacy laws around the word, consent too often provides companies with what professor Elettra Bietti aptly calls a "free pass" to use data in an enormous number of ways.[114]

(b) Limits on AI Data Collection

On the flip side, consent requirements can thwart the collection of personal data for AI models even when they have significant benefits. Additionally, scraping can assist researchers and journalists. Technology journalist Julia Angwin points out that for journalists to examine "how despots, trolls, spies, marketers and hate mobs are weaponizing tech platforms or being enabled by them," journalists need "access to large quantities of public data . . . to understand whether an event is an anomaly or representative of a larger trend."[115] For AI data gathering across the internet, obtaining express individual consent would be a daunting challenge, if not impossible.

The GDPR doesn't contain an exception for publicly available information. The only way that organizations can gather data under the GDPR is to have one of six lawful bases to gather the data about a data subject: (1) consent; (2) necessary for a contract; (3) necessary to comply with a legal obligation; (4) necessary to protect a person's vital interests; (5) necessary for the public interest; and (6)

---

[111] GDPR, art. 4(11) (requiring consent to be "freely given, specific, informed and unambiguous indication of the data subject's wishes").

[112] Florencia Marotta-Wurgler, *Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts,"* 78 U. Chi. L. Rev. 165, 168 (2011) (study demonstrating that requiring people to click an "I agree" box next to terms only increased readership by 1%).

[113] Solove, *Murky Consent, supra* note X, at X.

[114] Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn,* 40 Pace L. Rev. 308, 313 (2020).

[115] Julia Angwin, "The Gatekeepers of Knowledge Don't Want Us to See What They Know," N.Y. Times (July 14, 2023).

necessary for legitimate interests and not "overridden by the interests or fundamental rights and freedoms of the data subject."[116]

Under the GDPR, large companies could find ways to obtain consent from their millions or billions of users. But small companies without a large user base need to gather their data from sources they don't control and where they lack the ability to obtain consent. These small companies would lack the volume of data necessary to train AI models.

In *HiQ Labs v. LinkedIn*, LinkedIn blocked HiQ from scraping personal data from its users' profiles. HiQ argued that this blocking was anti-competitive, and the court agreed.[117] Further litigation continued, and the case ultimately settled. Although the court was wrong to allow companies to flaunt privacy protections in the name of competition, there certainly is a valid concern that if companies can only use data they have, then the big companies will have a tremendous advantage in the development of AI.

Under the GDPR, the most plausible legal basis would be legitimate interests.[118] But the GDPR is also restrictive with legitimate interests, making the use of this basis difficult and not at all assured, as it would depend upon the specific uses of the AI.

If the GDPR ends up extensively restricting AI data collection in the EU or if privacy laws of certain jurisdictions bar data collection, this could have a skewing effect. For example, if training data about people from the EU or a particular country were excluded, an AI model might be skewed toward reflecting people from places where data can be more freely collected. AI algorithms will emphasize the cultural practices and behaviors of the people whose data it is trained on.

C. DATA GENERATION

1. Inference

AI affects privacy by making inferences about people. Inference occurs through a phenomenon I term the "aggregation effect" – the fact that assembling numerous small bits of personal data can uncover significantly more than their individual contributions suggest.[119] Advances in modern computing have greatly amplified the ability to detect underlying patterns in data. AI algorithms can

[116] GDPR art. 6.

[117] HiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019). For background about the clash between privacy and anti-competition law, see Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, Yale L.J. Forum (Jan. 18, 2021).

[118] Magali Feys, Herlad Jongen, & Gary LaFever, *Legal Basis Requirements for AI,* LinkedIn (July 17, 2023), https://www.linkedin.com/pulse/legal-basis-requirements-ai-gary-lafever/.

[119] SOLOVE, THE DIGITAL PERSON, *supra* note X, at 44-47.

readily infer new insights about individuals.

As Alicia Solow-Niederman points out, AI algorithms generate new data about people in ways that people don't expect: "[M]achine learning facilitates an *inference economy* in which organizations use available data collected from individuals to generate further information about both those individuals and about other people."[120] For example, people may think they are revealing innocuous data, but this data can be used to infer sensitive information about their health, religion, political beliefs, sex life, and other highly personal matters.[121] As Solow-Niederman notes, people will find it difficult (if not impossible) "to predict which bits of data are significant. This result disempowers individuals who seek to shield their personal data yet can no longer know what needs protecting."[122]

(a) The Problem of Data Generation

Privacy laws provide individuals with notice about the data *gathered* about them, but they often fail to provide notice about data *generated* about them. From the individual's standpoint, it doesn't matter whether data was gathered or generated; the ultimate result is that data about them is known that they didn't expect or agree to. Making inferences can lead to severe privacy violations when the data generated uncovers details people prefer not to reveal. This was highlighted in a well-known incident involving Target, a large retail store chain. Target developed an algorithm to identify pregnant women based on their shopping patterns. The goal was to recognize pregnancy early on and encourage these women to see Target as their go-to retailer for baby products. In a notable case, a man complained to Target about his teenage daughter receiving numerous baby-related advertisements, thinking they were sent in error. However, he soon discovered that his daughter was indeed pregnant.[123]

Target's algorithm identified pregnancy by recognizing specific buying patterns: purchases of unscented products, vitamins, and cotton balls were common among pregnant customers.[124] What is quite concerning about the algorithm is that it could infer sensitive health data from relatively innocuous data. Additionally, the data the algorithm used to make its inference was hard to anticipate.

Inference thus upends the traditional picture for how people manage their own

---

[120] Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 Nw. L. Rev. 357 (2022).

[121] Solove, *Data Is What Data Does, supra* note X, at X.

[122] Solow-Niederman, *Inference Economy*, *supra* note X, at X.

[123] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times Magazine (Feb. 16, 2012); CHARLES DUHIGG, THE POWER OF HABIT: WHY WE DO WHAT WE DO IN LIFE AND BUSINESS 182-97, 209-10 (2012).

[124] CHARLES DUHIGG, THE POWER OF HABIT: WHY WE DO WHAT WE DO IN LIFE AND BUSINESS 194 (2012).

privacy. Machine learning algorithms are able to make so many surprising inferences that people have no control over what data organizations know.[125]

Inferences can cause harm not only when they are accurate, but even when they are wrong. AI makes inferences by matching an individual's profile with a vast dataset of others, identifying similarities in profiles. Thus inferences can cause harm whether they are correct or incorrect; accurate inferences might expose too much about people's private lives and inaccurate inferences might result in misguided judgments or decisions about people.

Privacy legislation tends to concentrate on the actual gathering of data rather than on the creation of data through inferential processes. While most privacy laws grant individuals the right to rectify their data or consent to its collection, they typically fall short in allowing individuals to challenge or rectify inferences derived from their data.[126]

As discussed earlier, the process of generating data through inferences essentially mirrors the act of data collection. A key principle of many privacy regulations is to restrict organizations to collecting only the personal data necessary for defined purposes. However, if organizations can create new data via inferences, then restrictions on data collection become somewhat illusory. Inference-generated data subverts public expectations and renders claims about limiting data collection misleading. Therefore, the law should treat data derived from inferences on an equal footing with collected data.

Unfortunately, privacy laws don't treat data generation the same as data collection. Many U.S. privacy laws focus on data collected from or about individuals.[127] Even under the GDPR, as Sandra Wachter and Brent Mittelstadt note, "inferences receive less protection under data protection law than other types of personal data provided by the data subject."[128]As Mireille Hildebrandt argues, EU law "builds on traditional ways of thinking about *data*, personal data and their possible abuse, without having a grasp on the new type of *knowledge* that is generated by data processing. The conclusion must be that even if data protection legislation were effective regarding personal data, it does not know how to deal with *patterns of correlated data*."[129]

---

[125] Solove, *Data Is What Data Does, supra* note X, at X.

[126] Matsumi, *The Failure of Rectification, supra* note X, at X.

[127] For example, the CCPA defines data collection as "'buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior." CCPA 1798.140 (f).

[128] Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 Colum. Bus. L. Rev. 494, 572 (2019).

[129] Mireille Hildebrandt, *Profiling and the Identity of the European Citizen, in* PROFILING THE EUROPEAN CITIZEN: CROSS-DISCIPLINARY PERSPECTIVES 303, 321 (Mirielle Hildebrandt & Seth Gutwirth eds. 2008).

While many privacy laws grant individuals rights to amend their data or consent to its collection, they seldom provide means to challenge or rectify inferences drawn from their data. Sandra Wachter and Brent Mittelstadt propose that privacy law should provide individuals with a "right to reasonable inferences."[130] They argue: "In cases where algorithms draw 'high-risk inferences' about individuals, this right would require the data controller to provide ex-ante justification to establish that the inference to be drawn is reasonable."[131]

Although a right to reasonable inferences would be a positive advancement for privacy law, it is far from enough. The power of AI to make inferences renders many provisions and goals of current privacy law moot. If new data can be inferred about people that they don't expect or consent to, the idea that people can be informed about the data collected about them and can decide what is known about them and how the data is used is obsolete. AI's vast power to make inferences starkly demonstrates the unworkability of the individual control model.

(b) End-Runs Around Privacy Protections

AI data generation can lead to end-runs around privacy protections. Privacy law has long protected confidential data, excluding it from being collected for certain decisions. For example, confidential data generated in professional relationships such as with doctors and lawyers is excluded from adjudicatory decisions in order to protect the confidentiality of these relationships. Even if the data could render the decision more accurate – even if it is crucial to establish truth at a trial – it is still excluded by privileges.[132] In another example, the federal Genetic Information Nondiscrimination Act (GINA) provides that employers may not "request, require, or purchase genetic information with respect to an employee or family member of the employee," except under certain exceptions.[133]

With its tremendous power to make inferences, however, AI technologies can generate personal data that otherwise would be excluded under confidentiality protections. AI can render protections of confidential data meaningless if inferences can be generated to navigate around them. Thus, privacy law must restrict using inferred data as an end-run around restrictions on using confidential data.

Additionally, AI can thwart the ability to de-identify personal data. As law professor Charlotte Tschider notes, AI can thwart various privacy laws that allow the use of de-identified personal data, such as HIPAA and the CCPA, by making

[130] Wachter & Mittelstadt, *Reasonable Inferences, supra* note X, at 500.

[131] *Id.* at 500-01.

[132] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 419-20 (8th ed. 2024).

[133] 42 USC § 2000ff.

it possible to re-identify the data.[134]

The problem of inferences requires a complete overhaul of privacy law; it is not an issue that can readily be patched. AI inferences demonstrate that attempts to protect privacy by regulating data gathering are insufficient; the law must also address data generation.

2. Malevolent Material

Beyond inferences, AI can generate a wide array of content. Some of this content can be quite harmful. AI chatbots can invent false facts about people, a phenomenon called "hallucination." In one instance, ChatGPT falsely stated that a professor was a sexual harasser.[135] AI can be used to facilitate "deep fakes" (realistic fake photos and videos about people).[136] In countless cases, deep fake porn videos are being made about people, mostly women, causing them immense harm.[137] A recent example involved the viral dissemination of deepfake sexually explicit images and videos of music star Taylor Swift.[138]

Compounding the problem is that many AI tools are available to the public, and anyone can use them for nefarious purposes. It is difficult to catch and punish the malicious users of AI, and there might be some First Amendment impediments as well as considerable time and expense for victims to pursue legal redress. Privacy laws should place responsibilities on the creators of AI tools to restrict harmful uses. But as with many technology products or services, the law has typically only weakly imposed responsibilities on their creators when people use them in harmful ways. AI will likely be a similar story.

With online platforms, for example, U.S. law prevents them from being held responsible for user content. The Communications Decency Act (CDA) Section 230 immunizes platforms for the content of their users: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[139] Although the text of Section 230 is narrow, courts interpret it broadly as a huge

---

[134] Charlotte A. Tschider, *AI's Legitimate Interest: Towards a Public Benefit Privacy Model,* 21 Hous. J. Health L. & Pol'y 125, 176 (2021).

[135] Pranshu Verma and Will Oremus, "ChatGPT Invented a Sexual Harassment Scandal and Named a Real Law Prof as the Accused," Wash. Post (Apr. 5, 2023).

[136] Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,* 107 Cal. L. Rev. 1753 (2019); Mary Anne Franks & Ari Ezra Waldman, *Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions*, 78 Md. L. Rev. 892 (2019).

[137] Jennifer Kite-Powell, "Deepfakes Are Here, Can They Be Stopped?" Forbes (Sept. 20, 2023); CITRON, FIGHT FOR PRIVACY, *supra* note X, at 38-39; Mary Anne Franks and Danielle Keats Citron, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform,* 2020 U. Chi. Legal F. 45 (2020).

[138] Blake Montgomery, "Taylor Swift AI Images Prompt US Bill to Tackle Nonconsensual, Sexual Deepfakes," The Guardian (Jan. 30, 2024).

[139] 47 U.S.C. § 230(c)(1).

grant of immunity to platforms for the speech of its users.[140] Section 230 originally aimed to ensure that a platform should not be liable as a publisher or speaker for information provided by others; it did not aim to eliminate distributor liability, which involves distributors of others' content being liable if they know or should know the content is defamatory or invasive of privacy.[141] Courts, however, have vastly broadened the scope of Section 230 to wipe out distributor liability in the name of free speech.[142] As law professor Danielle Citron has argued, the law not only protects sites for failing to do anything to stop harmful content but also protects sites that encourage and facilitate such content.[143] With the law's protection, these sites have proliferated. Citron notes: "More than 9,500 sites host user-provided nonconsensual intimate images, including up-skirt, down-blouse, and deepfake sex videos, and authentic intimate images."[144]

AI has the capacity to magnify fraud, cons, and swindling, amplifying this malignant activity. For example, in one case, a woman received a call from her daughter, who was crying: "Mom these bad men have me. Help me! Help me!" The kidnappers initially demanded that she wire $1 million to them or else they would harm her daughter. But the call was a fake. The daughter's voice was being impersonated with AI.[145]

AI tools are being released to the public with few guardrails, protections, or rules of use. The public is being armed with a powerful tool that can readily be weaponized to cause widespread harm to individuals or catastrophic harm to society.[146] Although sharing AI tools with the public can be democratizing, it can also be dangerous, as inevitably many people will misuse these tools.

AI can create new data security vulnerabilities. AI can help hackers and malevolent actors better carry out their attacks as well as perpetrate new more malicious scams. AI can assist in identifying vulnerabilities or writing malware.[147] With Generative AI, hackers can engage in "prompt injections," where they engineer inputs to "cause a large language model AI chatbot to

---

[140] *See* Zeran v. AOL, 129 F. 3d 327 (4th Cir. 1997); *see also* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 167-76 (8th ed. 2024).

[141] DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 149-160 (2007).

[142] SOLOVE, FUTURE OF REPUTATION, *supra* note _, at X. *See also* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014). For more background on Section 230, see JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019).

[143] CITRON, FIGHT FOR PRIVACY, *supra* note X, at 104.

[144] Danielle Keats Citron, *The Continued (In)visibility of Cyber Gender Abuse*, 133 Yale L.J. Forum 333, 347 (2023).

[145] Erum Salam, "US Mother Gets Call from 'Kidnapped Daughter' – But It's Really an AI Scam," The Guardian (June 14, 2023).

[146] *See* Philipp Hacker, Andreas Engel, and Marco Mauer, *Regulating ChatGPT and Other Large Generative AI Models* (May 12, 2023), https://doi.org/10.48550/arXiv.2302.02337.

[147] Chuck Brooks, "A Primer on Artificial Intelligence and Cybersecurity," Forbes (Sept. 26, 2023).

expose data that should be kept private."[148] Hackers could also poison training data to affect generative AI results.

Laws have long criminalized fraud, but digital crime can be quite hard to stop. Criminals can be anywhere, far outside the practical reach of local law enforcement. As AI tools find their way into unscrupulous hands, they will be used to victimize more people on a grander scale. The law has thus far been woefully inadequate at protecting victims of identity theft and fraud in the digital age.[149]

For data security problems, the law remains in desperate need of reform. Many privacy laws rest address data security heavily through data breach notification, which involves requirements for organizations that have a data breach to inform regulators and affected individuals.[150] Unfortunately, breach notification isn't a vaccine or a cure; it's just a notification about a disease. At best, breach notification provides greater transparency about data breaches, which is a good thing, but not something that fortifies data security.

Data security law, with limited exceptions, typically focuses narrowly on the organizations that are breached and fails to assign responsibility to all the responsible parties. Preoccupied with the aftermath of breaches, the law neglects necessary preventative measures and fails to allocate responsibilities to those who are in a position to both prevent and mitigate the effects of data breaches.[151] The law fails to hold all the actors that contribute to data breaches accountable.[152] Creators of AI tools can unleash a pandora's box of perils and yet evade responsibility for these damage that ensues. AI underscores the need for new approaches in the law.

3. Simulation

AI can be deceptive, disguising that it is AI. People might think they are interacting with a human but are really engaging with a machine. Simulation of a human can be a form of deception. Simulating a human makes humans respond differently because there are different moral considerations when interacting with a human than with a machine. As law professor Frank Pasquale argues, "When chatbots fool the unwary into thinking that they are interacting with humans, their programmers act as counterfeiters, falsifying features of actual human existence to increase the status of their machines."[153]

---

[148] Trend Micro, "Top 10 AI Security Risks According to OWASP," (Aug. 15, 2023), https://www.trendmicro.com/en_vn/ciso/23/h/top-ai-risks.html.

[149] Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability,* 54 Hastings L.J. 1227 (2003).

[150] DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT (2022).

[151] *Id.*

[152] *See id.* at 81-110.

[153] FRANK PASQUALE, NEW LAWS OF ROBOTICS: DEFENDING HUMAN EXPERTISE IN THE AGE OF AI 8

Modern AI tools are increasingly able to pass the Turing test. The test, devised by Alan Turing in 1950, looks to whether humans can decipher if they are interacting with another human or a machine.[154] For Turing, the question of whether machines could be intelligent was "meaningless." What mattered was how well machines could imitate humans, and he proposed an "Imitation Game" where a questioner would ask questions to a concealed human and machine and determine which was which.[155]

The Turing test, however, assumes it doesn't matter whether the machine is actually intelligent; as long as the machine fools people into believing it is human, this is sufficient. In essence, the Turing test assumes reality doesn't matter as long as a simulation appears to be real.

But there are major differences between simulation and reality. Simulation is fictional; it is intentionally constructed by humans with particular aims and assumptions and for particular purposes. The issue of whether machines have genuine intelligence matters because it affects how we might ethically and legally assign responsibility for its output, decisions, and behavior.

Additionally, if AI were truly intelligent, this affects whether we should give it any recognition of agency. In Isaac Asimov's novella, *Bicentennial Man,* a robot seeks and wins his freedom, then engages in litigation the right to be transformed into a human.[156] True intelligence commands at least a consideration of moral and legal recognition of personhood as well as moral and legal responsibility for one's actions. But the AI of today is just a tool and remains solely the responsibility of its creators and users.

AI can also be manipulative even if we know it is a simulation. A simulation can be so convincing that we become so beguiled by its verisimilitude that we find it hard to resist behaving as if it were real. We might know it isn't real, but it still might trigger our emotions and entice us to behave in different ways. For example, we might forge greater bonds of trust with simulated intelligence than we would with a less anthropomorphic machine. For example, in the movie *Her* (2013), a man falls in love with an AI persona. He knows she is not real, but he is nevertheless bewitched by the simulation. The movie raises questions about whether this relationship was a good one. The protagonist is jolted back to reality when he learns that the AI persona is talking to many other people simultaneously and says she is in love with hundreds of them. Even full transparency about the fact we're engaging with AI can't fully address this problem.

(2020).

[154] Alan Turing, *Computing Machinery and Intelligence*, 59 Mind 433 (1950).

[155] *Id.*

[156] ISAAC ASIMOV, THE BICENTENNIAL MAN AND OTHER STORIES (1976).

Privacy laws must regulate human-AI interactions. People should know if they are interacting with AI or a real human. Beyond requiring transparency about the involvement of AI, the law must recognize that in certain circumstances, AI is not just any computer code. Human simulation can be immensely powerful in ways that other machine interactions are not.

D. DECISION-MAKING

AI is often used to make decisions about people that are based on personal data or have effects on an individual's personal life. For example, AI tools are increasingly used in workplace hiring decisions, from evaluating resumes to conducting analysis on video interviews.[157] AI is in widespread use in criminal detention and sentencing decisions.[158] AI decision-making is different from human decision-making and raises many concerns that warrant regulatory attention.

1. Prediction

AI tools are often employed to make predictions about the future. As legal scholar Hideyuki Matsumi and I have noted, algorithmic predictions are increasingly being made and their consequences and harms are not fully appreciated.[159]

Algorithmic predictions are made based on patterns in past data. There are two assumptions behind algorithmic predictions: (1) that history repeats itself and what happened in the past will happen again in the future; and (2) that people who have similar characteristics or behavior patterns are likely to be similar in other things.

Machine learning algorithms and AI technologies are used not only to make inferences about the past and present but also to forecast future events.[160] Predictions are a subset of inferences, but they are distinct enough from inferences about the past and present that they warrant special focus and treatment.

Algorithmic predictions do more than just forecast the future; they also shape

---

[157] AJUNWA, THE QUANTIFIED WORKER, *supra* note X, at 138-70. HILKE SCHELLMANN, THE ALGORITHM: HOW AI DECIDES WHO GETS HIRED, MONITORED, PROMOTED & FIRED, & WHY WE NEED TO FIGHT BACK NOW 83-128 (2024).

[158] BERNARD E. HARCOURT, AGAINST PREDICTION: PROFILING, POLICING, AND PUNISHING IN AN ACTUARIAL AGE 41-45 (2007); Jessica M. Eaglin, *Predictive Analytics' Punishment Mismatch*, 14 I/S: A J. of L. & Pol'y, 87, 100-01 (2017).

[159] Hideyuki Matsumi & Daniel J. Solove, *The Prediction Society: AI and the Problems of Forecasting the Future,* work-in-progress.

[160] Hideyuki Matsumi, *Predictions and Privacy: Should There Be Rules About Using Personal Data to Forecast the Future?*, 48 Cumb. L. Rev. 149 (2018);

it.[161] These algorithms function by analyzing extensive datasets and employing statistical methods to predict future outcomes. There is an increasing reliance on algorithmic forecasts in matters concerning human behavior, such as assessing whether criminal defendants should be detained pre-trial due to flight risk, determining the length of criminal sentences based on recidivism, evaluating creditworthiness based on loan repayment histories, and predicting the potential success of job applicants.[162]

These algorithmic decisions have significant impacts on individual opportunities and liberties. People may face job rejections due to health predictions, be subjected to heightened airport security based on terrorism risk assessments, and encounter law enforcement actions through predictive policing tactics.[163]

(a) Threat to Human Agency

Despite their potential advantages, algorithmic predictions pose a serious challenge to individual agency. Algorithmic forecasts limit people's ability to forge their own paths.

Decisions derived from predictive models challenge the principles of due process.[164] Justice traditionally dictates that individuals should not face penalties for actions they have not committed. However, predictive models enable judgments and potential repercussions based on actions that individuals have not undertaken and may never undertake. As Professor Carissa Véliz contends, "by making forecasts about human behavior just like we make forecasts about the weather, we are treating people like things. Part of what it means to treat a person with respect is to acknowledge their agency and ability to change themselves and their circumstances."[165]

This issue was evident in the case of *Wisconsin v. Loomis*, where an algorithmic system known as COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) assessed the defendant as a high risk for reoffending, leading to a longer sentence.[166] The defendant argued that his due process rights were violated since the algorithm's prediction was based on data from others,

---

[161] Matsumi & Solove, *The Prediction Society, supra* note X, at X.

[162] *Id.*

[163] ANDREW GUNTHRIE FERGUSON, THE RISE OF BIG DATA POLICING (2017); Albert Meijer & Martijn Wessels, *Predictive Policing: Review of Benefits and Drawbacks*, 42 Int'l J. Pub. Admin. 1031, 1031 (2019); Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 Harvard L. & Pol'y Rev. 15, 15-18 (2016); Orla Lynskey, *Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing,* 15 Int'l J. L. in Context 162, 167 (2019); Lindsey Barrett, *Reasonably Suspicious Algorithms: Predictive Policing at the United States Border,* 41 N.Y.U. Rev. L. & Soc. Change 132 (2017).

[164] CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016).

[165] Carissa Véliz, *If AI Is Predicting Your Future, Are You Still Free?* Wired (Dec. 27, 2021).

[166] Wisconsin v. Loomis, 881 N.W.2d 749 (Wis. 2016).

not his specific behavior. Although the Wisconsin Supreme Court dismissed this argument, noting that the judge was not obliged to follow the algorithm's recommendation, the judge still relied on it.[167]

Studies indicate a tendency for individuals to defer to algorithmic conclusions. Ben Green points out that "people cannot reliably balance an algorithm's advice with other factors, as they often overrely on automated advice and place greater weight on the factors that algorithms emphasize."[168]

Compounding the concerns in the *Loomis* case was the refusal to disclose how the COMPAS algorithm functioned, with its creator citing trade secrets.[169] Subsequent analysis of COMPAS revealed bias against black defendants.[170]

The 2022 sci-fi movie *Minority Report* illustrates a chilling dystopian world where police use a system to foresee crimes and apprehend individuals before they commit any actual offense. Algorithmic predictions have a similar effect – they are used to preemptively judge people before they have acted, undermining the right of individuals to make their own choices and punishing them for deeds not yet committed. As Katrina Geddes argues, "algorithmic prediction effectively punishes the underlying individual for membership of a statistical group."[171] People should be evaluated on the basis of their own actions, not on what others do.

(b) Fossilizing the Past

Algorithmic predictions do not function as a crystal ball providing a definitive view of the future. These predictions are, in reality, probabilities derived from historical data, which often contain inherent biases, discrimination, inequalities, and privileges. Decisions made on the basis of these algorithmic predictions tend to solidify past patterns. For instance, historical racial discrimination has led to disproportionately higher arrest and conviction rates for black individuals.[172] When such data is input into algorithms, it results in predictions of increased recidivism rates for these populations, thereby imposing harsher sentences. As a result, algorithmic predictions have the potential to perpetuate and project existing inequalities and biases into the future.[173]

---

[167] Ben Green, *The Flaws of Policies Requiring Human Oversight of Government Algorithms*, 45 Computer Law & Security Rev. 1, 7 (2022).

[168] *Id.* at 9.

[169] For a critique of the use of trade secrets in this context, see Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System,* 70 Stan. L. Rev. 1343 (2017).

[170] Jeff Larson et al., *How We Analyzed the COMPAS Recidivism Algorithm*, at 1 (2017), https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

[171] Geddes, *Legal Subject, supra* note X, at 31.

[172] Jessica M. Eaglin, *Constructing Recidivism Risk*, 67 Emory L.J. 59, 72 (2017).

[173] Sandra G. Mayson, *Bias In, Bias Out*, 128 Yale L.J. 2218, 2224 (2019); Anupam Chander, *The Racist Algorithm?*, 115 Mich. L. Rev. 1023, 1036 (2017); Pauline T. Kim, *Manipulating Opportunity,* 106 Va. L. Rev. 867, 870 (2020) (AI "systems are likely to distribute information about future opportunities in ways that reflect existing inequalities and may reinforce historical

Algorithmic predictions often overlook the distinct qualities and personal narratives of individuals, focusing instead on statistical norms.[174] However, history is frequently shaped by the unexpected, challenging the reliance on these predictions. Nassim Nicholas Taleb calls these unexpected phenomena "black swans" – named after the black swans that Europeans encountered after discovering Australia. Before this, Europeans believed all swans were white. Taleb references this event to emphasize the importance of modesty in making predictions. He suggests that while we might be adept at forecasting routine events, the ability to predict the extraordinary is significantly limited.[175]

(c) Self-Fulfilling Prophecies

Predictions often become self-fulfilling prophecies, especially when they prompt actions that reinforce the anticipated outcome. For instance, a prediction indicating that individuals with certain characteristics are more prone to criminality could result in increased policing of such individuals. This heightened scrutiny might lead to more arrests and convictions—not necessarily because the prediction is accurate, but because law enforcement is disproportionately targeting those who fit the profile.[176]

Predictions about human behavior are not just made for the sake of understanding; they are tools for action. AI is used in decision-making processes and interventions. As a result, algorithmic predictions empower organizations to shape, control, and monetize human behavior more effectively.

(d) Beyond Accuracy

Algorithmic predictions present difficulties fitting into existing privacy law frameworks. The main vehicle privacy laws provide for addressing predictions is to provide individuals with a right to correction. Beyond the problem of relying too heavily on individual control, a right to correct erroneous data, but this right does not work for predictions, which are difficult to evaluate as either accurate or inaccurate since they pertain to events that have not yet occurred.[177] Algorithmic predictions are neither true nor false, as their veracity is only established once they manifest in reality. Consider, for instance, the impossibility of an individual disproving a prediction that they will commit a crime in the future. The truthfulness of this prediction can only be definitively assessed posthumously, making it virtually unchallengeable in the present.

---

patterns of disadvantage.").

[174] Geddes, *Legal Subject, supra* note X, at 5.

[175] NASSIM NICHOLAS TALEB, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE xvii, 149, 138, 149 (2007).

[176] GANDY, CHANCE, *supra* note X, at 124-25.

[177] Hideyuki Matsumi, *Right to Rectification,* draft on file with author.

When regulating decision-making with (or augmented by) AI algorithms, the law has often resorted to focusing on process. In the *Loomis* case, for example, the court mandated only basic procedural safeguards, primarily focusing on greater transparency regarding the use of algorithmic predictions and ensuring human participation. However, as Alicia Solow-Niederman points out, such steps are largely superficial and only serve to project an "appearance of legality."[178] Rather than settling for cosmetic process solutions that superficially enhance the situation, the law should robustly address the challenges posed by algorithmic predictions. This involves ensuring that these predictions adhere to fairness and align with the broader values of society. Broadly, the law should aim to ensure *fair decisions*. Decisions about people should be made fairly, considering the complete situation and their individual actions and characteristics, and treating them as unique individuals with agency.

2. Decisions and Bias

AI decisions are often touted as superior to human ones. As Orly Lobel observes, "AI can be a force for debiasing, and it can provide early detection of discrimination and abuse."[179] According to Cass Sunstein, algorithms can "prevent unequal treatment and reduce errors." In contrast to humans, algorithms "do not use mental shortcuts; they rely on statistical predictors, which means that they can counteract or even eliminate cognitive biases."[180]

Human decision-making is riddled with challenges. People are prone to biases, rely on a limited scope of experiences, and tend to be slow and inefficient in their decision processes. Emotional influences and irrational elements often sway their choices. Additionally, humans can act impulsively and are subject to various cognitive biases and heuristics, which can lead to flawed decisions.[181]

But AI algorithms have significant flaws that throw into question whether they are better than human decision-making.[182] Algorithms alter decision-making by emphasizing quantifiable data at the expense of qualitative factors. While this can be advantageous, it also comes with significant, often overlooked costs. Quantifying human lives is fraught with difficulty.[183] AI decisions currently do not incorporate emotions, morality, or value judgments, all crucial in decisions affecting human welfare. There is a risk of overly focusing on automated

[178] Alicia G. Solow-Niederman, *Algorithmic Grey Holes,* 5 J. Law & Innovation 116, 124 (2023).

[179] ORLY LOBEL, THE EQUALITY MACHINE: HARNESSING DIGITAL TECHNOLOGY FOR A BRIGHTER, MORE INCLUSIVE FUTURE (2022).

[180] Cass R. Sunstein, *Governing by Algorithm? No Noise and (Potentially) Less Bias*, 71 Duke L.J. 1175, 1177 (2022).

[181] *See* DANIEL KAHNEMAN, THINKING FAST AND SLOW (2011); Solove & Matsumi, *Awful Humans, supra* note X, at X.

[182] Jenna Burrel and Marion Fourcade, *The Society of Algorithms,* 47 Annual Rev. Sociology 213, 222-23 (2021) (arguing that AI algorithms are not necessarily better than human decision-makers).

[183] Solove & Matsumi, *Awful Humans, supra* note X, at X.

elements while disregarding ethical dimensions.[184]

What makes bias emerging from AI more potentially more dangerous and pernicious than bias in individual humans is that AI tools can be used broadly, systematizing bias and also cloaking it in the guise of a neutral technology. Bias harbored by specific individuals—even many individuals—can still be overcome when some individuals deviate and decide without a particular bias. This is how social change occurs, first starting with a few people and then spreading over time. But AI can quickly systematize bias, making it more pervasive and inescapable, snuffing out the stirrings of societal improvement.

(a) Biased Training Data

AI algorithms are far from unbiased because they are fueled with data from society, where bias abounds. As Meredith Broussard writes, "*[A]ll data is dirty*. All of it."[185] Law professor Sandra Mason argues that "a racially unequal past will necessarily produce racially unequal outputs."[186] If input data is biased, then outputs will be biased. She argues that if more black people have been arrested than white people based on past data, "then a predictive analysis will project it to happen more frequently to black people than to white people in the future."[187]

The problem with biased data was evident when Amazon tried to create an algorithm for hiring in technical roles, only to find the outcomes heavily biased towards male candidates. This bias emerged because the algorithm was trained on a decade's worth of hiring data, which itself was skewed towards males due to pre-existing hiring biases.[188] The quality and impartiality of automated decisions are directly influenced by the data they are based on, and this data is seldom free from bias.

Technologist Cathy O'Neil argues that algorithmic models "are constructed not just from data but from the choices we make about which data to pay attention to—and which to leave out. Those choices are not just about logistics, profits, and efficiency. They are fundamentally moral."[189] As law professor Jesscia Eaglin argues, data used by algorithms is not just found but selected and crafted with particular value judgments. For example, Eaglin notes that the input data in algorithmic recidivism risk assessment systems hinges on "policy questions

---

[184] Solove & Matsumi, *Awful Humans, supra* note X, at X.

[185] MEREDITH BROUSSARD, ARTIFICIAL UNINTELLIGENCE: HOW COMPUTERS MISUNDERSTAND THE WORLD 103 (2018).

[186] Sandra G. Mayson, *Bias In, Bias Out*, 128 Yale L.J. 2218, 2224 (2019).

[187] *Id. See also* Anupam Chander, *The Racist Algorithm?*, 115 Mich. L. Rev. 1023, 1036 (2017) ("Algorithms trained or operated on a real-world data set that necessarily reflects existing discrimination may well replicate that discrimination."); Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 Cal. L. Rev. 671, 682 (2016).

[188] AJUNWA, THE QUANTIFIED WORKER, *supra* note X, at 83-84.

[189] CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016).

about who should be considered a risk and how much risk society tolerates."[190] The data used by AI algorithms might be perceived to be neutral, but it is normative.

In what she terms the "input fallacy," law professor Talia Gillis argues that merely trying to cleanse information about a person's race, religion, or other protected characteristics from input data will not lead to clean outputs. She observes that "information about a person's protected characteristics is embedded in other information about the individual, so that a protected characteristic can be 'known' to an algorithm even when it is formally excluded."[191]

(b) Novel Forms of Discrimination

AI Algorithms have the potential to introduce novel forms of discrimination, focusing on attributes they deem significant. [192] These traits may not be the traditionally recognized bases of discrimination like race, gender, or age, but could include characteristics often viewed unfavorably, such as being short, overweight, or bald. Some criteria used by algorithms might appear arbitrary, relying on unusual correlations. For instance, if an algorithm finds a link between eye color and poor job performance, it might disfavor this trait. This leads to the creation of new, undesirable categories, systematically affecting individuals. We could witness the rise of a new kind of inequality where people face discrimination based on immutable characteristics. This form of inequality may be less visible due to the complexity of algorithms, making it harder to detect and address.

(c) Addressing Bias

The law must address biased decisions, which are difficult to eradicate. As Anupam Chander argues, because "the real-world facts, on which algorithms are trained and operate, are deeply suffused with invidious discrimination," it should be no surprise that the algorithms produce discriminatory results.[193] He contends that "We must design our algorithms for a world permeated with the legacy of discriminations past and the reality of discriminations present."[194]

Biased decisions are unfair decisions, and they must be examined substantively for bias. Process-based requirements are helpful, but they are not sufficient to

---

[190] Jessica M. Eaglin, *Constructing Recidivism Risk*, 67 Emory L.J. 59 (2017).

[191] Talia B. Gillis, *The Input Fallacy*, 106 Minn. L. Rev. 1175 (2022).

[192] Tal Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 Seton Hall L. Rev. 995, 1012 (2017).

[193] Anupam Chander, *The Racist Algorithm?*, 115 Mich. L. Rev. 1023 (2017); *see also* Elizabeth E. Joh, *Feeding the Machine: Policing, Crime Data, & Algorithms*, 26 Wm. & Mary Bill Rts. J. 287, 289 (2017) ("Every action—or refusal to act—on the part of a police officer, and every similar decision made by a police department, is also a decision about how and whether to generate data.").

[194] *Id.*

address the problem. The law cannot address unfair decisions without looking at the substance of these decisions.[195]

3. Automation

To love, to feel, to empathize,
Are the things that make us alive,
And though AI may be wise,
It's still just an artificial hive.

– ChatGPT

AI involves automated data processing. The nature of such processing raises privacy issues because of the way that automation shapes and distorts data and the way it treats individuals. Automation changes the nature and effects of decision-making about people. Sometimes, it can produce changes for the better, but it also has tradeoffs and can lead to diminished decisions that fail to respect people's unique personhood.

(a) Quantification and Depersonalization

When data is collected to train algorithms, it must be ingested. The data must be standardized; idiosyncratic data will be refined out. Nonquantifiable data is not readily usable. As Dan Burk contends, uniting data elements for quantitative analytical tools "necessarily strip[s] away much of the unique formatting and context of the original source. To reconfigure otherwise incompatible data, analytical processing imposes a radical decontextualization on the data, paring away extraneous information and meanings."[196] When qualitative data is removed, leaving just quantifiable data, the nuance, texture, and uniqueness of individuals is lost.[197] Decisions are being made about people based on a distorted picture of them.

While automation seeks to replicate human decision-making, it often struggles to capture the subtleties and irregularities of human thinking and behavior.[198] Automated decisions can lack the personalization necessary for the diverse and complex scenarios of human life. While large-scale quantitative data can reveal broad trends and patterns, it often glosses over individual differences and unique characteristics. As statistics pioneer Lambert Adolphe Jacques Quetelet

[195] Andrew D. Selbst and Solon Barocas argue that FTC jurisprudence regarding "unfair" trade practices can address discrimination. The unfairness inquiry can focus on the substance of a decision, not just the procedure. Andrew D. Selbst and Solon Barocas, *Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law*, 171 U. Pa. L. Rev. _ (2024).

[196] Dan L. Burk, *Algorithmic Legal Metrics*, 96 Notre Dame L. Rev. 1147 (2020).

[197] DANIEL J. SOLOVE, THE DIGITAL PERSON, *supra note X, at* 49.

[198] Andrea Roth, *Trial by Machine*, 104 Geo. L.J. 1245 (2016) (discussing the pathologies of automation in criminal adjudication).

remarked: "The greater the number of individuals observed, the more do individual particularities, whether physical or moral, become effaced, and leave in a prominent point of view the general facts, by virtue of which society exists and is preserved."[199]

Data that cannot be easily quantified is often overlooked by automated systems. This process involves distilling the intricate and varied experiences of life into more straightforward, pattern-based formats. The rich and complex information yielded by human experiences must be simplified. Nuanced differences that defy quantification or standardization are often lost in this process. Yet, these nuances are crucial, as human judgment frequently relies on them. Life's richness often lies in its uniqueness and unpredictability, and many vital aspects of human experience resist easy quantification.[200] As Julie Cohen declares, people are not "reducible to the sum of their transactions, genetic markers, and other measurable attributes."[201]

The stakes with AI decision-making are enormous because they can operate so efficiently on a massive scale. AI algorithms have the potential to solidify and systematize existing biases and prejudices.[202] Solon Barocas and Andrew Selbst have highlighted a critical issue in the realm of automated decision-making: biases from past decisions can become codified into formalized rules, leading to systematic impacts.[203] Not only biases but any other shortcomings of AI decision-making can become amplified and ingrained.

(b) Regulating Automation

Addressing automation presents a significant challenge for the law. The most robust law that regulates automated decision-making is the GDPR, which provides individuals with a "right not to be subject to a decision based solely on automated processing, including profiling."[204] Individuals have the "at least the right to obtain human intervention . . . to express his or her point of view and to contest the decision."[205] As Meg Leta Jones notes, the philosophy behind the GDPR is that "treating an individual in a wholly automated way, or to provide only automated treatment, is to dehumanize the individual, because a machine

---

[199] Lambert Adolphe Jacques Quetelet quoted in CHRIS WIGGINS AND MATTHEW L. JONES, HOW DATA HAPPENED: A HISTORY FROM THE AGE OF REASON TO THE AGE OF ALGORITHMS 26 (2023).

[200] DANIEL J. SOLOVE, THE DIGITAL PERSON, *supra note X,* at 49; Burk, *Algorithmic Legal Metrics*, *supra note X,* at 1158.

[201] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1405 (2000).

[202] Margot E. Kaminski & Jennifer R. Urban, *The Right to Contest AI,* 121 Colum. L. Rev. 1957, 1981 (2021).

[203] Solon Barocas & Andrew D. Selbst, Big Data's Disparate Impact, 104 Cal. L. Rev. 671, 682 (2016),

[204] GDPR, *supra* note X, art. 22(1) ("The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.").

[205] Id. at art 22(3).

can only treat a human in a computational manner."[206]

In the U.S., the CCPA provides individuals with some rights regarding automated decision-making, such as a rights to opt out, to learn about the algorithmic logic, and to know about the likely outcome.[207] A few other state laws address automated decision-making, mainly by providing opt out rights.[208]

A major limitation in the GDPR's approach to automation is that its protections are limited to decisions made "solely" through automation. However, many automated processes involve some level of human intervention, rendering these specific protections inapplicable. The GDPR's Article 22 on automated decision-making is limited to solely automated decisions because so many decisions today are hybrid human and machine, and this would extend the GDPR into countless decisions – a slippery slope because the GDPR Article 22 might extend to all decisions involving data or calculations, even where a person just glanced at a statistic. But drawing the line at *solely* automated decisions is far too limiting. A more plausible line might be drawn where automation plays a material role in a decision.

The GDPR's protections for automated processes are far from enough. A big component of the GDPR's treatment of automated processes is to require human involvement. But for the increasing number of hybrid decisions, made by a combination of humans and machines, humans are already involved. What is needed are more substantive requirements about the quality of automated decision-making and measures to address the problems of automation.

While various laws attempt to manage automated decisions through transparency requirements, such transparency often fails to be truly insightful. The complexity of the algorithms that drive these decisions is typically beyond the average person's comprehension. Merely understanding the logic behind these decisions is insufficient, as they rely on personal data from millions, which cannot be disclosed without breaching privacy norms. Without access to the data on which these algorithms are trained, evaluating certain automated decisions becomes a challenging, if not impossible, task.

(c) Integrating Human and Machine Decision-Making

Privacy laws must address how to integrate human and machine decision-making. The GDPR regulates automated processing in Article 22, but it is limited

[206] Meg Leta Jones, *The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood*, 47 Soc. Stud. Sci. 216 (2017).

[207] CCPA, Cal. Civ. Code § 1798.185(a)(16) (mandating that the Attorney General issue regulations that businesses disclose "meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.").

[208] Thomas, "Privacy Law Deluge," *supra* note X.

to "solely" automated data processing.[209]

Article 22 further provides that when a data subject challenges a decision based solely on automated processing, the data controller must implement safeguards for an individual's "rights and freedoms and legitimate interests," and provide for "the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."[210]

Unfortunately, as many commentators have pointed out, human involvement is not an effective cure for problems with algorithmic decision-making.[211] As Rebecca Crootof, Margot Kaminski, and Nicholson Price observe, a "hybrid system" consisting of human and machines could "all too easily foster the worst of both worlds, where human slowness roadblocks algorithmic speed, human bias undermines algorithmic consistency, or algorithmic speed and inflexibility impair humans' ability to make informed, contextual decisions."[212] According to Margot Kaminski and Jennifer Urban, humans often harbor "automation bias" which "creates overconfidence in machine decisions."[213] Humans often struggle to effectively evaluate automated decisions, frequently deferring to algorithms and overlooking errors. Unfortunately, the GDPR lacks specific guidelines on how humans should review automated decisions.[214]

As Ben Green aptly points out, human and machine decision-making processes differ significantly, making their integration akin to mixing oil and water. Algorithmic decision-making prioritizes consistency and strict rule adherence, whereas human decision-making involves "flexibility and discretion." Calls for human oversight of algorithms overlook the "inherent tension" between these two approaches.[215]

Automation undoubtedly offers efficiency but at the cost of producing oversimplified and distorted judgments that fail to capture the complexities of real-life situations. The issue does not lie with technology itself but with the hasty assumption that automation is superior to human decision-making and neutral. The problem stems from how technology is perceived. Technology should not be seen as a panacea for the flaws in human decision-making, nor

---

[209] GDPR art. 22

[210] GDPR art. 22

[211] *See, e.g.,* Kaminski, *Binary Governance*, *supra* note X (humans in the loop will not improve automated decision-making); Kiel Brennan-Marquez, Karen Levy & Daniel Susser, *Strange Loops: Apparent Versus Actual Human Involvement in Automated Decision Making*, 24 Berkeley Tech. L.J. 745 (2019) (humans in the loop can end up being there merely for appearances); Aziz Z. Huq, *Constitutional Rights in the Machine-Learning State*, 105 Cornell L. Rev. 1875, 1908–10 (2020) (humans in the loop often do not improve the accuracy of decisions).

[212] Rebecca Crootof, Margot E. Kaminski & W. Nicholson Price II, *Humans in the Loop*, 76 Vand. L. Rev. 429, 468 (2023).

[213] Kaminski & Urban, *The Right to Contest AI*, *supra note X, at* 1961.

[214] Crootof, Kaminski, & Price, *Humans in the Loop*, *supra* note X, at 437.

[215] Ben Green*, The Flaws of Policies Requiring Human Oversight of Government Algorithms*, 45 Computer Law & Security Rev. 1, 12 (2022).

should humans be viewed as a cure for the limitations of automated decision-making. Instead, the primary objective of the law should be to ensure that decisions are fair.

E. DATA ANALYSIS

AI can facilitate social control through surveillance and identification to a staggering degree. As Mustafa Suleyman writes, "The ability to capture and harness data at an extraordinary scale and precision; to create territory-spanning systems of surveillance and control, reacting in real time . . . would rewrite the limits of state power so comprehensively that it would produce a new kind of entity altogether."[216]

1. Surveillance

In 1791, philosopher Jeremy Bentham conceived the "Panopticon," a prison layout characterized by cells arranged around a central watchtower. This design aimed for maximum efficiency, reducing the need for numerous guards to oversee prisoners. In the Panopticon, inmates lived in constant apprehension of being observed, which led to docility and compliance.

Centuries later, Michel Foucault recognized the extension of panoptic power beyond physical prison structures.[217] He observed that society was constructing a self-imposed prison through the proliferation of surveillance technologies, enabling concealed observers to monitor individuals from remote locations.

Today, the trajectory toward a panoptic society has accelerated. Surveillance cameras have become ubiquitous, multiplying rapidly and being monitored by remote bureaucrats. The internet tracks virtually every aspect of people's actions, recording an extensive digital trail. Julie Cohen has astutely pointed out that the consequences of our surveillance society are constraining free thought and democracy. They erode the boundaries of expression and intellectual exploration, influencing how individuals think and behave.[218]

Additionally, surveillance provides government with broad powers which are readily susceptible to abuse. Surveillance extends further than a mere physical search as it captures a person's actions, social interactions, and potentially every word and deed. Surveillance has the capacity to gather an extensive range of data that may exceed its initial scope. With prolonged observation, individuals could potentially be observed engaging in illegal or unethical behavior, providing a

---

[216] MUSTAFA SULEYMAN, THE COMING WAVE: TECHNOLOGY, POWER, AND THE 21ST CENTURY'S GREATEST DILEMMA 192 (2023).

[217] MICHEL FOUCAULT, DISCIPLINE AND PUNISH (Alan Sheridan trans., Vintage Books, 2d ed. 1995) (1977); *see also* OSCAR T. GANDY, THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993) (describing the panoptic effects of the emerging digital economy).

[218] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stanford Law Review 1373 (2000).

pretext to punish or discredit them.

AI technologies enable mass surveillance at unprecedented levels. Already, many societies have an extensive infrastructure of video and audio surveillance, geolocation tracking, and data gathering. But the footage, audio recordings, feeds, tracking data, and other data require analysis. As Bruce Schneier astutely argues, "AI changes the ballgame because it can readily analyze the data captured by surveillance technologies."[219] Schneier distinguishes between surveillance (gathering data) and spying (analysis of data). Spying takes considerable human labor, and this limits how extensive spying can be. But with AI, Schneier notes, data "will all be searchable, and understandable, in bulk."[220] There aren't enough people to sift through all the immense quantities of data gathered, not enough people to listen to all audio captured or watch all surveillance video footage. But AI can do all this. Schneier writes:

> Summarization is something a modern generative A.I. system does well. Give it an hourlong meeting, and it will return a one-page summary of what was said. Ask it to search through millions of conversations and organize them by topic, and it'll do that. Want to know who is talking about what? It'll tell you.[221]

Surveillance is a problem that pre-dates AI, and the law has generally failed to deal with it effectively. AI will amplify the harms of surveillance to an alarming degree.

2. Identification

AI facilitates identification based on eyes, face, gait, voice, and other physical characteristics. AI can detect distinctive patterns in so much of what people do and say that it can enable a myriad of identification methods.

When individuals are easily identifiable, it amplifies the government's power, which can enhance social order but also has the potential to be used as an instrument of oppression. Identification makes it easier for governments to target and detain individuals they view unfavorably.

The danger of misuse is significantly heightened when identification becomes systematic and covert. As political scientist Richard Sobel notes, identification systems have historically been used for social control and discrimination.[222] For instance, slaves were forced to carry identification papers for travel, the Nazis

---

[219] Bruce Schneier, *The Internet Enabled Mass Surveillance. A.I. Will Enable Mass Spying,* Slate, Dec. 4, 2023.

[220] *Id.*

[221] *Id.*

[222] Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U. J. Sci. & Tech. L. 37, 39 (2002).

used ID cards to locate Jews, and the Rwandan genocide was facilitated by a system of identifiers. Government officials could misuse these records for inappropriate surveillance. Data becomes a versatile tool for those in power, adaptable to any current impulse. A notable example is the Census Bureau's use of 1940 census data to support the internment of Japanese-Americans during World War II.[223]

Throughout the world, societies are swiftly moving towards this reality without adequate foresight or safeguards. AI will grease the wheels as we race in this direction. Recent developments in facial recognition are already propelling us toward this dystopian future. Facial recognition makes surveillance more potent because it enables surveillance footage to be readily linked to particular individuals. Efforts by law enforcement and corporations to implement facial recognition technology have been met with challenges, including inaccuracies and public backlash, leading to the abandonment of many such initiatives.[224] Despite these setbacks, the technology has persisted and evolved, much like a fungus thriving in the dark.

AI facial recognition poses a significant threat to personal anonymity. As Woodrow Hartzog and Evan Selinger write, "facial recognition is the perfect tool for oppression."[225]

As with other privacy problems affected by AI, the main impact of AI is amplification. AI represents the perfection of the surveillance society – the step that threatens to turn pervasive surveillance into totalizing control. The law has long failed to provide the appropriate control and oversight of surveillance and identification. AI threatens to make this failure all the more tragic.

3. Interpretation and Deciphering

AI can also facilitate the interpretation of data in the government's possession. For example, suppose the government located an encrypted file and decrypted it with an AI tool. Orin Kerr contends that encryption fails to create a Fourth Amendment reasonable expectation of privacy because "the Fourth Amendment regulates government *access* to communications, not the *cognitive understanding* of communications already obtained."[226] Under this reasoning, when the government finds items with a person's DNA, the government can, without Fourth Amendment protection, analyze the DNA. AI will provide the

[223] See ERIK LARSON, THE NAKED CONSUMER: HOW OUR PRIVATE LIVES BECOME PUBLIC COMMODITIES 53-54 (1992).

[224] HILL, YOUR FACE BELONGS, *supra* note X.

[225] Woodrow Hartzog & Evan Seligner, *Facial Recognition Is the Perfect Tool for Oppression,* Medium (Aug. 2, 2018), https://medium.com/@hartzog/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08fofe66; Lindsey Barrett, *Ban Facial Recognition Technologies for Children—and for Everyone Else*, 26 B.U. J. Sci. & Tech. L. 223 (2020).

[226] Orin S. Kerr, The Fourth Amendment in Cyberspace: Can Encryption Create a Reasonable Expectation of Privacy?, 33 Conn. L. Rev. 503 (2001).

government with new capabilities of discovering data about people, evading the oversight and limitation protections of the Fourth Amendment.

Kerr provides an example of the absurdity of requiring a warrant for law enforcement to decipher "messy handwriting or understanding Hegel."[227] Clearly, the Fourth Amendment shouldn't be triggered whenever the police do any kind of data analysis, because this could extend to nearly every aspect of an investigation, which is akin to figuring out a puzzle. If the government finds a note written in French, it is silly to require a Fourth Amendment warrant to translate it into English.

AI, however, turns the dial up from these examples to an incredibly sophisticated capacity to interpret and decipher. Just as there is a danger of a slippery slope to absurd situations like messy handwriting, AI creates a slippery slope in the other direction. For example, the government could gather de-identified data from the internet and re-identify it with AI. The government could use AI systems to infer extensive data about a person from data it possesses or finds online. Because of this, the law can't adhere to simple absolute rules like the one Kerr supports. A line must be drawn somewhere, and it will be difficult because there is rarely a precise point for a line when dealing with issues involving degree and magnitude.

This discussion captures the essence of many problems AI poses for the law. AI cranks up the volume to an extent that significantly alters the situation. AI often confounds the law with the paradox of the heap: removing a grain of sand doesn't mean the heap is no longer a heap. If grains are removed one by one, there never appears to be a good point to say that sand isn't a heap.

4. Limitation and Oversight

The concerns raised by AI use with government surveillance and data gathering are best addressed by fixing the severe shortcomings in existing law. Due to a series of unfortunate decisions of the U.S. Supreme Court, Fourth Amendment protection against government surveillance and data gathering has been decimated. Currently, the government has few limitations on gathering data from the internet or buying data from commercial entities.[228]

In a line of cases known as the "Third Party Doctrine," the U.S. Supreme Court has ruled that there is no reasonable expectation of privacy for data disclosed to third parties. For example, in *United States v. Miller*, where federal agents obtained the defendant's bank records without notification. The Court

[227] *Id.*

[228] Matthew J. Tokson, *Government Purchases of Private Data,* forthcoming Wake Forest L. Rev. (2023), draft at p. 4, https://ssrn.com/abstract=4574166 ("Police officers can generally purchase items available to the public without constitutional restriction."); Orin Kerr, Buying Data and the Fourth Amendment, Hoover Inst., Stan. Univ. 1, 11 (Nov. 2021), https://www.hoover.org/sites/default/files/research/docs/kerr_webreadypdf.pdf.

determined that there was no reasonable expectation of privacy for financial records held by a bank because the data was "revealed to a third party."[229] In *Smith v. Maryland,* the Court found no reasonable expectation of privacy in the use of pen registers since individuals because the data was conveyed to the phone company.[230] Although *Carpenter* curtails the reach of the Third Party Doctrine to some extent, the Court did not overturn it.[231]

Ultimately, the law allows the government wide latitude to engage in surveillance, as well as gather and purchase data. The Fourth Amendment currently provides few restrictions on how long the government can store personal data and how they can analyze it.[232] The Fourth Amendment protects against unreasonable searches and seizures and says little about what happens to data after the government has acquired it.[233] In other words, in the way it has often been interpreted and applied, the Fourth Amendment focuses mainly on data collection and neglects data analysis.[234] AI increases the power of what the government can do with the data it collects.

If the Fourth Amendment or statutory protection were to try to limit the government's analysis of the data it possesses, a major challenge would be where to draw the line. Certainly, law enforcement officials must be able to analyze data in order to investigate crime. A line must be drawn somewhere, though, because AI takes data analysis to hitherto unprecedented levels.

The law ought to ensure that the government can't use AI systems in ways that create undue harms or risks. There must be constant independent oversight as well as a set of rules for use and accountability for misuse.

Currently, though, with AI tools, law enforcement officials are like kids in a toy store who can buy anything they want and use it however they want with scant oversight or accountability. The law's problems with regulating government surveillance, data gathering, and use of technology make the law woefully unprepared for AI. Although the Fourth Amendment was drafted in a broad and open-ended way, prohibiting "unreasonable searches and seizures," it has been interpreted in narrow and shortsighted ways that have rendered it inapplicable to an enormous amount of problematic privacy-invasive activities through

---

[229] United States v. Miller, 425 U.S. 435, 443 (1976).

[230] Smtih v. Maryland, 442 U.S. 735, 737 (1979).

[231] United States v. Ellison, 462 F.3d 557 (6th Cir. 2006) (searching through law enforcement databases isn't a Fourth Amendment violation).

[232] United States v. Ellison, 462 F.3d 557 (6th Cir. 2006) (searching through law enforcement databases isn't a Fourth Amendment violation); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy,* 75 S. Cal. L. Rev. 1083, 1166 (2002) ("Once information is collected, the Fourth Amendment's architecture of oversight no longer applies.").

[233] William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 Harv. L. Rev. 842, 848 (2001) ("Fourth Amendment law regulates the government's efforts to uncover information, but it says nothing about what the government may do with the information it uncovers.").

[234] Daniel J. Solove, *Data Mining and the Security-Liberty Debate,* 74 U. Chi. L. Rev. 343 (2008).

technology. As law professor Fred Cate notes, "despite the proliferation of government data mining programs, Congress has enacted no legislation to provide a legal framework for how such programs are to be undertaken, to provide redress for innocent people harmed by them, or to specify how privacy is to be protected in the process."[235]

F. OVERSIGHT, PARTICIPATION, AND ACCOUNTABILITY

1. Transparency

A central pillar of privacy law is transparency: Organizations must be transparent about the data they collect and how they use it. Transparency poses great challenges for AI. As Frank Pasquale argues, many algorithms are "secret" – and their use is resulting in our living in a "black box society" where important decisions about our lives are unexplained and unaccountable.[236] Margot Kaminski notes that "transparency of some kind has a clear place in algorithmic accountability governance."[237] However, she notes that there are disputes about what, precisely, should be transparent. Should there be rather barebones notice about the existence of automated processes? Should there be transparency about the algorithmic code – its logic? Or should the data that algorithms are trained on be disclosed?

The General Data Protection Regulation (GDPR) introduces certain rights related to automated processing, which include a degree of algorithmic transparency.[238] Under these provisions, data controllers are required to inform individuals about the use of automated decision-making, provide meaningful insight into the logic of these processes, and explain the potential consequences.

For transparency to be truly meaningful, automated decisions need to be comprehensible. This is a challenge with machine learning algorithms, as the decisions they make can be intricately complex.[239] Suleyman notes that AI algorithms are "not explainable" because "[y]ou can't walk someone through the decisionomaking process to explain precisely why an algorithm produced a

---

[235] Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 Harv. Civ. R. Civ. L. L. Rev. 435, 461 (2008).

[236] FRANK PASQUALE, THE BLACK BOX SOCIETY: THE HIDDEN ALGORITHMS THAT CONTROL MONEY AND INFORMATION 218 (2015); Charlotte A. Tschider, *Beyond the "Black Box,"* 98 Denv. L. Rev. 683, 699 (2021); W. Nicholson Price, *Black-Box Medicine,* 28 Harv. J.L. & Tech. 419, 421 (2015).

[237] Margot E. Kaminski, *The Right to Explanation, Explained*, 34 Berkeley Tech. L.J. 199 (2019).

[238] GDPR art. 13, § 2(f), at 40–41; id. art. 14, § 2(g), at 41–42 (requiring that data subjects be informed about "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."); *see also id.* art. 15, § 1(h), at 43.

[239] Carolin Kemper, *Kafkaesque AI? Legal Decision-Making in the Era of Machine Learning*, 24 Intell. Prop. & Tech. L.J. 251, 275 (2020) ("The intricate design of ML algorithms, their complex learning technique, and the large amounts of data influencing the algorithm's structure, render it difficult to trace why a specific result was obtained.").

specific prediction."[240] AI algorithms are dynamic, and they rely on the collective data of numerous individuals. To fully understand a particular decision made about an individual, one would need to know not just their personal data and the algorithm's logic, but also the data of others that the algorithm has processed. Revealing this broader data set, however, risks infringing on the privacy of other individuals.

Even when these decisions are made transparent, they can still be problematic and potentially unfair. Thus, while transparency is a crucial aspect of data protection, it alone is insufficient to address the myriad issues associated with algorithmic decision-making.[241] Additional measures are needed to ensure these systems operate fairly and without causing harm.

Moreover, even with transparency, most individuals are not equipped to evaluate complex algorithms. In many cases, understanding an algorithm requires access to the training data it utilizes, which often isn't readily available or producible, let alone comprehensible.[242] This data often can't be disclosed without violating people's privacy. The volume of data in these data sets is far too vast for individuals to handle.

Additionally, many algorithms are dynamic, continually learning and evolving based on new data, necessitating ongoing assessment, which is practically unfeasible for most individuals. This complexity further underscores the limitations of current privacy rights in addressing the broader implications of data use and algorithmic decision-making. Even experts struggle to understand why algorithms generate certain outputs.[243] As technologist Joy Boulamwini notes: "A major challenge of neural networks is that during the training process computer scientists do not always know exactly why some weights are strengthened and others are weakened."[244]

Algorithmic transparency can be thwarted by trade secret protections. As law professor Charlotte Tschider observes, "explaining how an AI decision is made will likely destroy an algorithm's trade secret status, depending on the extent of the required disclosure."[245] Trade secrecy can be used by the creators of algorithms to shield them from scrutiny. In the *Loomis* case, the trade secrets of the company that developed the recidivism risk analysis tool COMPAS

---

[240] SULEYMAN, THE COMING WAVE, *supra note X, at* 143.

[241] Devin R. Desai & Joshua A. Kroll, *Trust But Verify: A Guide to Algorithms and the Law*, 31 Harv. J.L. & Tech. 1, 64 (2017) (transparency is not enough protection for problems with algorithms); Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 Fordham L. Rev. 1085, 1088 (2018) ("Explanations of technical systems are necessary but not sufficient to achieve law and policy goals.").

[242] Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 Md. L. Rev. 439, 445 (2020).

[243] Tschider, *AI's Legitimate Interest, supra* note X, at 130.

[244] JOY BOULAMWINI, UNMASKING AI: MY MISSION TO PROTECT WHAT IS HUMAN IN A WORD OF MACHINES 53 (2023).

[245] Tschider, *Black Box, supra* note X, at 711.

prevented defendants from being able to analyze the tool.[246] Law professor Rebecca Wexler criticizes the use of trade secrets in criminal cases because it places "pure financial interests on par with life and liberty."[247]

Ultimately, transparency will be a challenge with AI, but it should not be abandoned. Privacy laws should avoid relying too heavily on transparency. But transparency is valuable, and even though training data can't be disclosed, details about it can be disclosed. AI algorithms can be vetted by researchers and experts.

2. Due Process

As mentioned earlier, AI can threaten individual due process. As Danielle Citron argues, "Automation jeopardizes the due process guarantees of meaningful notice and opportunity to be heard."[248] Along with Frank Pasquale, Citron argues that greater due process is needed in credit scoring, "[p]rocedural protections should apply not only to the scoring algorithms themselves (a kind of technology-driven rulemaking), but also to individual decisions based on algorithmic predictions (technology-driven adjudication)."[249]

Margot Kaminski and Jennifer Urban note that in the U.S., "regulatory proposals directed at algorithmic decision-making have largely ignored calls for individual due process in favor of system-wide regulation aimed at risk mitigation."[250] They argue that in the EU, the GDPR provides individuals with a right to challenge AI decisions: "The GDPR incorporates both systemic governance measures and various individual rights for data subjects: transparency, notice, access, a right to object to processing, and, for those subject to automated decision-making, the *right to contest* certain decisions."[251] The U.S. should have similar protections. According to Kate Crawford and Jason Schultz, a neutral party should examine individual complaints.[252]

Although the law still must provide room for individuals to have a voice and adjudicate complaints, the law must avoid resting the bulk of its protections on individual challenges, as this puts too much onus on individuals and adheres too much to the unworkable individual control model.

---

[246] Wisconsin v. Loomis, 881 N.W.2d 749 (Wis. 2016).

[247] Rebecca Wexler, *Life, Liberty, and Trade Secrets*, 70 Stan. L. Rev. 1343, 1402 (2018).

[248] Danielle Keats Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249 (2007).

[249] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).

[250] Kaminski & Urban, *The Right to Contest AI*, *supra note X, at* X.

[251] *Id.* at X.

[252] Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. Rev. 93 (2014).

3. Stakeholder Involvement

Scholars raise concerns about the potential development of AI in an exclusive manner, as key decisions often lack the involvement of all relevant stakeholders. Far too often, AI systems are having profound effects on underrepresented groups, especially when used by the government.

For instance, in the case of pretrial detention algorithms, law professor Ngozi Okidegbe highlights that individuals from economically disadvantaged backgrounds and racial minorities may be excluded from the governance of these algorithms, which are "opaque or non-inclusive of the oppressed populations that are most likely to interact with it."[253]

Alicia Solow-Niederman contends that the "AI field is missing the active public voice necessary for a democratically accountable governance model. . . . Any negotiation will occur in an unregulated market, without democratically accountable coordination or enforceable checks on commercial profit motives."[254]

Because AI affects privacy of countless stakeholders and because AI algorithms are often trained on personal data, there is a justification for the law imposing an obligation on the creators of such algorithms to consider the input of stakeholders as represented by groups and associations.

4. Accountability

Another approach to regulating AI involves the implementation of governance and accountability mechanisms. Privacy laws often incorporate such measures, which encompass the appointment of privacy officers, the conduction of privacy impact assessments, the establishment of written policies and procedures, transparency in data practices, documentation, and more. These mechanisms, which have proven effective in the context of privacy, could also be adapted to regulate AI.

As Pauline Kim argues, "Technical tools alone cannot reliably prevent discriminatory algorithms because the causes of bias often lie not in the code, but in broader social processes."[255] She further contends that "Avoiding discriminatory outcomes will require awareness of the actual impact of automated decision processes, namely, through auditing."[256]

According to Talia Gillis and Josh Simons, accountability "should be the central

[253] Ngozi Okidegbe, *The Democratizing Potential Of Algorithms?*, 53 Conn. L. Rev. 739 (2022).
[254] Alicia Solow-Niederman, *Administering Artificial Intelligence,* 93 S. Cal. L. Rev. 633 (2020).
[255] Pauline T. Kim, *Auditing Algorithms for Discrimination*, 166 U. Pa. L. Rev. Online 189, 202 (2017).
[256] *Id.*

aim of all approaches to governing decision-making using machine learning." They elaborate: "Structures of accountability can incentivize institutions to develop decision-making procedures with more care, consider a broad range of interests and perspectives, and evaluate more kinds of risk and possible harms."[257] Gillis and Simons aptly argue that "Part of the value of accountability is that it changes the conduct of those with power because they know that conduct will have to be justified."[258]

A key question to be resolved with accountability – one that remains fraught and underexamined in privacy law – is where the primary responsibility with implementing accountability measures should rest. For example, should organizations do self-audits? Should government regulators do audits? Should independent third parties do audits?

Many privacy laws delegate the responsibility for implementing the majority of accountability and governance mechanisms to companies. Professor Ari Waldman slams this approach as woefully ineffective: "Transparency, impact assessments, paper trails, and the traditional accountability mechanisms they support do not address the gaps in the underlying social and political system that not only lays the groundwork for algorithmic decision-making but sees its proliferation, despite its biases, errors, and harms, as a good thing."[259] Waldman proposes that instead of a compliance model, "regulators, assisted by independent academic experts, [should] audit algorithmic decision-making code for its adherence to social values."[260]

Auditing and review must have a substantial independent component. Otherwise, organizations will struggle to be restrained when the reward for ignoring risks is high. Regulation must balance a tightrope between overly trusting organizations to manage themselves with avoiding micromanaging and requiring permission for everything an organization might do. Ultimately, there must be a mix of internal and external accountability mechanisms. Organizations must face meaningful consequences for the harms and risks they create; too often they don't, creating incentives not to take legal duties seriously.

5. Enforcement and Remedies

AI presents challenges for remedies when privacy laws are violated. When AI algorithms are created by improperly gathering data, it becomes difficult to untwine the data from the algorithm. The algorithm has already "learned" from the data. Tiffany Li labels this effect an "algorithmic shadow" – the "persistent

[257] Talia B. Gillis and Josh Simons, *Explanation < Justification: GDPR and the Perils of Privacy*, Pa. J. L. & Innovation (2019).
[258] *Id.*
[259] Ari Ezra Waldman, *Power, Process, and Automated Decision-Making*, 88 Fordham L. Rev. 613 (2019).
[260] *Id.*

imprint of the data that has been fed into a machine learning model."[261] Thus, the remedy of data deletion fails to "eliminate the algorithmic shadow" – there is "no impact on an already trained model."[262] The result is a lack of incentive to avoid unlawful data collection; the benefit becomes baked into the algorithm, so companies come out ahead even if they are required to delete the data they pilfered.

One remedy that is increasingly being used is algorithmic destruction. For example, in *In re Everalbum, Inc.,* the FTC ordered a company to delete "any models or algorithms" developed with data it had improperly collected.[263] However, Li argues that the remedy of algorithmic destruction can be too severe and might "harm small startups and discourage new market entrants in technology industries."[264] Additionally, it is one thing for the FTC to order a small company to delete an algorithm, but what about a gigantic company such as Open AI? It is hard to imagine the FTC or any regulator ordering the deletion of a hugely popular algorithm with a multi-billion dollar value.

Moreover, is this remedy viable for instances where only some data was improperly gathered? Deleting an entire AI system because one person's data was improperly included would be overkill. Nevertheless, algorithmic destruction could be an appropriate remedy where most of the data was improperly gathered or the algorithm is causing considerable harm.

Another challenge is that the money and investment in AI is at epic proportions. The prize for developing successful AI tools involves extraordinary riches. Fines and enforcement rarely are sufficient to counterbalance such gains. The result is skewed incentives, where a company can take a shortcut by breaking the law and be rewarded with a great treasure, then later apologize and pay back a small fraction of the gain. AI entrepreneurs know the maxim: *Better to ask for forgiveness than permission.*[265]

Ultimately, enforcement will be a considerable challenge with AI. The incentives to "move fast and break things" will be quite high. Rarely will enforcers issue a penalty that can overcome such incentives when they become so strong.

---

[261] Tiffany C. Li, *Algorithmic Destruction*, 75 SMU L. Rev. 479, 482 (2022).

[262] *Id.* at 498.

[263] In re Everalbum, Inc. (2022).

[264] Li, *Algorithmic Destruction, supra* note X, at 505.

[265] For information about this maxim, see Fred Shapiro, *Quotes Uncovered: Forgiveness, Permission, and Awesomeness,* Freakonomics Blog (June 24, 2010), https://freakonomics.com/2010/06/quotes-uncovered-forgiveness-permission-and-awesomeness/.

CONCLUSION

> And yet, we cannot halt the march of time,
> Nor stay the progress of the tech we make,
> We must find ways to keep our lives sublime,
> And not allow our privacy to break.
>
> – ChatGPT

AI affects privacy in many ways, though often in ways that do not create radically new problems as much as remix and amplify existing ones. For privacy, AI's challenges are far from unexpected; they are steps along a path toward a long-predicted future.

Current privacy laws fall woefully short of addressing AI's privacy challenges. AI puts pressure on many of the weakest parts of privacy law. Privacy law's wrong approaches and other unfixed flaws are especially ill-suited for AI.

Substantial reform of privacy law is long overdue. Policymakers are concerned about AI, and a window appears to have opened where new approaches to regulation are being considered. Hopefully, this will present the opportunity to take privacy law in a new direction. To adequately regulate AI's privacy problems, the longstanding difficulties and wrong approaches of privacy law must be addressed.