RULES FOR ROBOTS: CONSTITUTIONAL CHALLENGES WITH THE AI BILL OF RIGHT'S PRINCIPLES REGULATING AUTOMATED SYSTEMS

*Melany Amarikwa**

INTRODUCTION

A few years ago, conversations about artificial intelligence ("AI") were confined to the pages of books and the ivory towers of academia. Now, even older generations know that AI makes many of the decisions in their lives. The heightened public awareness around AI has generated exciting conversations about its potential to push society into the future but it has also raised concerns about AI's safety and inherent fairness. These concerns raises the following question: Can I trust a "robot" or automated system that makes decisions on my behalf?

As the use of AI by federal agencies continues to grow, concerns have been raised about the potential for "corporate capture of public power."[1] As many government agencies lack the expertise and resources to develop their own AI models, they rely on private companies to create them,[2] leading to questions about bias and privacy safeguards in automated systems. These concerns add to the larger conversation about the trustworthiness of AI decision makers in our daily lives.

Research has validated fears by demonstrating how government agencies' initial use of AI is not to be trusted. A Yale Law School study found

https://doi.org/10.58112/jcl.26-4.6

* J.D. Candidate, 2024, University of Pennsylvania Law School; B.A., 2019, University of California, Berkeley. I am grateful to Professor Cynthia L. Dahl for her invaluable guidance and mentorship. I would also like to thank the editors of the University of Pennsylvania Journal of Constitutional Law for their efforts in bringing this article to publication.

1 *See* Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J. L. & TECH. 103, 109 (2018) ("The risk is that the opacity of the algorithm enables corporate capture of public power. When a government agent implements an algorithmic recommendation that she does not understand and cannot explain, the government has lost democratic accountability, the public cannot assess the efficacy and fairness of the governmental process, and the government agent has lost competence to do the public's work in any kind of critical fashion.").

2 *Id.* at 103 ("In the public sector, the opacity of algorithmic decision making is particularly problematic, both because governmental decisions may be especially weighty and because democratically elected governments have special duties of accountability.").

that responses to Freedom of Information ("FOI") requests are inadequate to enable "meaningful public oversight of the use of algorithms."[3] Consequently, these automated systems are making judgments impacting the public without public oversight. Additionally, researchers at Carnegie Mellon found that a Pennsylvania child welfare system's algorithmic Family Screening Tool made "more racially disparate decisions than workers," and workers had to intervene to correct these algorithmic biases.[4]

The Biden Administration responded to the concerns surrounding AI by unveiling the Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People ("AI Bill of Rights") in October of 2022.[5] The AI Bill of Rights has five principles that aim to guide the creation and use of automated systems: Safe and Effective Systems, Algorithmic Discrimination Protections, Data Privacy, Notice and Explanation, and Human Alternatives, Consideration, and Fallback.[6] Although the AI Bill of Rights is not a legally binding document,[7] it has the potential to influence courts, lawmakers, and private companies, with the Biden Administration's Executive Order on AI ("Executive Order on AI") and the Office of Management and Budget draft guidance ("OMB Guidance") borrowing

3 MEDIA FREEDOM & INFORMATION ACCESS CLINIC, YALE LAW SCHOOL, ALGORITHMIC ACCOUNTABILITY: THE NEED FOR A NEW APPROACH TO TRANSPARENCY AND ACCOUNTABILITY WHEN GOVERNMENT FUNCTIONS ARE PERFORMED BY ALGORITHMS iii (2022).

4 *See* Logan Stapleton et al., *Extended Analysis of "How Child Welfare Workers Reduce Racial Disparities in Algorithmic Decisions"* (2022) https://loganstapleton.com/wp-content/uploads/2022/04/Extended_Analysis__How_Child_Welfare_Workers_Reduced_RaciaR_Disparities_in_Algorithmic_Decisions.pdf [https://perma.cc/YCR3-R3WY].

5 *See generally* Press Release, The White House, What They Are Saying: White House Blueprint for an Ai Bill Of Rights Lauded As Essential Step Toward Protecting the American Public (Oct. 17, 2022), https://www.whitehouse.gov/ostp/news-updates/2022/10/17/what-they-are-sayingwhite-house-blueprint-for-an-ai-bill-of-rights-lauded-as-essential-step-toward-protecting-the-american-public/ [https://perma.cc/5SRQ-HS4P].

6 *See* BLUEPRINT FOR AN AI BILL OF RIGHTS MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE, THE WHITE HOUSE 5–7 (laying out the five principles central to the AI Bill of Rights) (Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf [https://perma.cc/2CFK-JJAQ] [hereinafter "AI BILL OF RIGHTS"].

7 *See* AI BILL OF RIGHTS, *supra* note 6, at 2 ("The Blueprint for an AI Bill of Rights is non-binding and does not constitute U.S. government policy. It does not supersede, modify, or direct an interpretation of any existing statute, regulation, policy, or international instrument.").

from the AI Bill of Rights.[8] As Secretary of State Antony J. Blinken stated, "government is constantly playing catch-up when it comes to technology" and the regulation of AI is no exception.[9] Given the AI Bill of Rights' role in shaping the future of regulations for automated systems, a deeper analysis of its legal implications is necessary for both public laws and private policies.

In this Comment, I argue that implementing certain principles of the AI Bill of Rights into laws and regulations could potentially violate the First and Fifth Amendments. While existing guidelines like the Fair Information Practice Principles are inadequate for regulating automated systems, the AI Bill of Rights is positioned to shape future regulation. By highlighting these challenges, I aim to offer guidance on how lawmakers may implement robust legislation that addresses AI concerns.

In Part I, I provide a brief background of the development of the Fair Information Practice Principles and the AI Bill of Rights. The U.S. Department of Health, Education, and Welfare Advisory Committee report, Records, Computers, and the Rights of Citizens, recognized the potential harm that computers could bring to personal privacy. These guidelines served as the foundation for subsequent data privacy legislation and regulation, including the Fair Information Practice Principles. Through an analysis of this significant moment in privacy law, this Comment aims to explore the potential trajectory of the AI Bill of Rights under the Biden Administration. I conclude the Section by providing an overview of the ways the AI Bill of Rights has already taken shape in the administration's policy agenda.

In Part II, I examine potential constitutional challenges that may arise if the AI Bill of Rights' principles are incorporated into future laws, specifically

---

8 WHITE HOUSE, EXECUTIVE ORDER ON THE SAFE, SECURE, AND TRUSTWORTHY DEVELOPMENT AND USE OF ARTIFICIAL INTELLIGENCE 3 (2023) [hereinafter "EXECUTIVE ORDER ON AI"]; *see also* Press Release, The White House, OMB Releases Implementation Guidance Following President Biden's Executive Order on Artificial Intelligence (Nov. 1, 2023), https://www.whitehouse.gov/omb/briefing-room/2023/11/01/omb-releases-implementation-guidance-following-president-bidens-executive-order-on-artificial-intelligence/ [https://perma.cc/9WS9-LDR3] ("OMB's proposed guidance builds on the Blueprint for an AI Bill of Rights and the AI Risk Management Framework by mandating a set of minimum evaluation, monitoring, and risk mitigation practices derived from these frameworks and tailoring them to context of the federal government.").

9 Secretary Antony J. Blinken on Advancing Technology for Democracy (Mar. 30, 2023), https://www.state.gov/secretary-antony-j-blinken-on-advancing-technology-for-democracy/ [https://perma.cc/T7WR-5K57].

addressing First and Fifth Amendment concerns. First, the Notice principle's documentation and outcome explanation requirements may raise First Amendment issues and potentially violate the Compelled Speech Doctrine. Lawmakers must carefully balance the need for transparency and accountability with the First Amendment and practical considerations when implementing the Notice principle. Second, the Data Privacy and Human Alternatives principles of the AI Bill of Rights may trigger the Takings Clause of the Fifth Amendment. To mitigate these concerns, laws seeking to apply the Data Privacy principle should follow the California Consumer Privacy Act's model and limit data restrictions to sensitive personal information. Laws that aim to implement the Human Alternatives principle may face fewer constitutional challenges compared to the Data Privacy principle laws. However, it is advisable to limit potential laws to opt-out options rather than mandating a human alternative.

The United States stands at a crossroads in the era of rapid technological change, where the exponential growth of AI has raised significant privacy concerns. Unlike other peer countries, the United States lacks a comprehensive federal privacy law, leaving the majority of American consumers at the mercy of private corporations.[10] AI has the potential to revolutionize the way society functions, much like the computer and internet did in the past. While the AI Bill of Rights represents a step in the right direction, it falls short of being a definitive solution to the well documented algorithmic privacy and bias issues.[11]

This Comment aims to address the shortcomings of the AI Bill of Rights and offers recommendations to lawmakers on how to prevent legal challenges that may arise from the application of its principles. By analyzing the gaps

---

10 A select few States, such as California, Connecticut, Colorado, Utah, and Virginia, have passed their own consumer data privacy laws. *State Laws Related to Digital Privacy*, NAT'L CONF. OF STATE LEGISLATURES (June 7, 2022), https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy [https://perma.cc/FGU9-Q54Z].

11 *See, e.g.,* Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 131 YALE L.J.F. 907 (2022) (arguing that African Americans are vulnerable to discriminatory oversurveillance, exclusion, and predation); *see also* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U.L. REV. ONLINE 793 (2021) (describing how a lack of cognizable harm prevents the remedy of privacy violations); *see also* Andrew Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109 (2017) (discussing the discriminatory impact of predictive policing systems); *see also* Melany Amarikwa, *Social Media Platforms' Reckoning: The Harmful Impact of TikTok's Algorithm on People of Color*, 29 RICH. J.L. & TECH. 69 (2023) (explaining the disproportionate risks social media algorithms pose to people of color).

in the current guidelines and exploring legal strategies for addressing them, this Comment intends to contribute to the ongoing efforts to ensure the responsible development and deployment of AI in the United States.

I. BACKGROUND

During the 1970s, the US hesitated to integrate computers into government work was met with hesitation amidst concerns about privacy and the use of personal data.[12] To address these concerns, the U.S. Department of Health, Education, and Welfare Advisory Committee published the Records, Computers, and the Rights of Citizens ("RCRC") report in 1973.[13] This report marked a pivotal moment in data privacy history, serving as a crucial milestone that laid the foundation for subsequent data privacy legislation and regulation.

One of the byproducts of the RCRC report was the development of the Fair Information Practice Principles ("FIPPs"), which established guidelines for handling personal data in online, which continue to shape privacy legislation.[14]

This Section provides an overview of the AI Bill of Rights, examines the FIPPs, and analyzes their potential impact on the AI Bill of Rights. Although the AI Bill of Rights has been criticized for lacking sufficient enforcement measures, it remains a significant step towards safeguarding individuals from the potential harm that may arise from automated systems.

A. THE DEVELOPMENT OF PRIVACY LAW

1. Records Computers and the Rights of Citizens

Before the modern AI revolution, the emergence of computers in the 1970s revolutionized American society. However, the advent of computers was not without its challenges. Concerns about these machines storing citizens' private data led the US Department of Health, Education, and

12 *Records, Computers, and the Rights of Citizens*, *infra* note 15, at x.

13 *Id.*

14 FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 3–5 (2000).

Welfare ("HEW") Advisory Committee to issue the RCRC report in 1973.[15] This Section explores the report's recommendations.

The RCRC report recognized the potential harm that computers presented to personal privacy.[16] The HEW Advisory Committee noted that existing government protections of personal privacy lacked a unified approach, rendering them ineffective in safeguarding individuals' privacy.[17] The report states, "[u]nder current law, a person's privacy is poorly protected against arbitrary or abusive record-keeping practices."[18]

To address these concerns, the HEW Advisory Committee proposed five guidelines for automated personal data systems.[19] First, record-keeping systems should be known to the public.[20] Second, individuals should have the right to know what information is being collected and what the data is being used for.[21] Third, individuals should have the right to prevent their data from being used for purposes outside of what they initially consented.[22] Fourth, there should be a method for individuals to correct or amend information about themselves.[23] Finally, organizations handling personal data must ensure data reliability and prevent data misuse.[24]

---

15 U.S. DEP'T OF HEALTH, EDUC., & WELFARE, DHEW PUB. NO. (OS)73-94, REP. OF SEC'Y ADVISORY COMM. ON AUTOMATED PERS. DATA SYS. (1973) v-viii [hereinafter *Records, Computers, and the Rights of Citizens*]; *see also* Electronic Privacy Information Center, FTC Commercial Surveillance & Data Security ANPR R11004, Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem at 152, (Nov. 2022) [hereinafter EPIC FTC Comment] ("Wary of the threats posed by the secret processing of personal information—and mindful of 'the principle of mutuality necessary for fair information practice'—the Advisory Committee on Automated Personal Data Systems set out baseline disclosure requirements for any organization maintaining such a data system.").

16 *See Records, Computers, and the Rights of Citizens*, *supra* note 15, at viii:

> The Secretary's Advisory Committee on Automated Personal Data Systems was established by former Secretary of Health, Education, and Welfare Elliot L. Richardson in response to growing concern about the harmful consequences that may result from uncontrolled application of computer and telecommunications technology to the collection, storage, and use of data about individual citizens.

17 *Records, Computers, and the Rights of Citizens*, *supra* note 15, at 34-35.

18 *Id.* at xx.

19 *Id.* at xx.

20 *See id.* at xx ("There must be no personal data record-keeping systems whose very existence is secret.").

21 *Id.*

22 *Id.*

23 *Id.*

24 *Id.* at xxi.

In summary, the RCRC report serves as a crucial milestone in the history of data privacy. Its recommendations on record-keeping systems, individual rights to information, data use, and data correction provided the foundation for subsequent data privacy legislation and regulation.[25]

2. Fair Information Practice Principles

The Fair Information Practice Principles ("FIPPs") developed as guidelines for handling personal data based in part on the recommendations outlined in the RCRC report. Although the HEW Advisory Committee's report only provided recommendations,[26] it had a significant impact on shaping both domestic and international privacy laws. In this Section, I introduce the FIPPs before discussing its impact on the AI Bill of Rights.

The FIPPs consist of eight privacy principles, namely data collection limitations, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[27] These principles aim to inform consumers about data collection practices and provide government regulators with a means to audit online services.[28]

Laws that draw on the FIPPs address the gathering, storage, utilization, and sharing of personally identifiable information ("PII"),[29] which the White House Office of Management and Budget defines as information that "can be used to distinguish or trace an individual's identity, . . . either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."[30] In summary, the FIPPs aim to protect

---

25 *See e.g.,* Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, Recital 32 (EU).

26 *Records, Computers, and the Rights of Citizens*, *supra* note 15, at iii.

27 OECD, RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, at 6-8,https://legalinstruments.oecd.org/public/doc/114/114.en.pdf [https://perma.cc/7LH6-FWHK].

28 *See* Yan Shvartzshnaider, Noah Apthorpe, Nick Feamster, & Helen Nissenbaum, *Analyzing Privacy Policies Using Contextual Integrity*, 18 SCIENDO 1 (2018) (assessing the efficacy of various privacy policy statements pertaining to online data collection using contextual integrity theory).

29 *See* Woodrow Hartzog, *Social Data*, 74 OHIO ST. L. J. 996, 999 (2013) (describing the general purposes and provisions of FIPPs).

30 OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB MEMORANDUM M-07-1616, SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (2007).

individuals' privacy by ensuring that their personal data is collected and used responsibly.

The FIPPs have significantly influenced data privacy legislation, with laws like the California Consumer Privacy Act and the Virginia Consumer Data Privacy Act adopting the FIPPs data minimization principle.[31] However, scholars argue that the FIPPs are outdated and ill-suited to protect consumers in the age of automated technologies and big data.[32] Woodrow Hartzog, a privacy and technology professor at Boston University School of Law, argues that the FIPPs have "painted us into a corner" and principles such as data minimization, transparency, choice, and access cannot adequately protect consumers in the algorithmic age.[33]

Hartzog is correct. The FIPPs, while useful in getting us to the present point, fail to protect consumers in the algorithmic age because they are limited to data privacy protection. While data privacy is an element of algorithmic accountability, it does not capture all the harms that may result from the use of automated systems. For example, consider a case in which a government agency uses an automated system to determine who may qualify for a government assistance program. Under the FIPPs, the government agency must comply with the eight principles which generally require it to limit its data collection and use, ensure data quality, get consent, and comply with transparency requirements. However, these principles fail to mitigate algorithmic discrimination issues as they do not require developers to ensure fair outcomes.

The Blueprint for an AI Bill of Rights addresses the shortcomings of automated systems by embracing and expanding on the elements of the

---

31 *See e.g.,* CALIFORNIA PRIVACY PROTECTION AGENCY, TITLE 11. LAW DIVISION 6. CALIFORNIA PRIVACY PROTECTION AGENCY CHAPTER 1. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS INITIAL STATEMENT OF REASONS 40 (2022); *see also* Ronald I. Raether Jr. et. al., *Virginia Consumer Data Protection Act Series: Part 4*, TROUTMAN PEPPER (Apr. 2021), https://www.troutman.com/insights/virginia-consumer-data-protection-act-series.html [https://perma.cc/7PL2-5WVY].

32 *See* Fred H. Cate, *The Failure of Fair Information Practice Principles, in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 343, 344 (Jane K. Winn ed., 2006) (discussing uneven enforcement of FIPPs); *see also* Kirk J. Nahra, *The Past, Present, and Future of US Privacy Law*, 51 SETON HALL L. REV. 1549, 1550 (2021) (arguing that privacy law is still in the early stages of development); *see also* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MARYLAND L. REV. 952, 953–956 (2017) (describing the history and highlighting the inadequacies of FIPPs).

33 Hartzog, *supra* note 32, at 953.

FIPPs.[34] By incorporating relevant elements of the FIPPs, the AI Bill of Rights seeks to provide a comprehensive framework that addresses privacy, civil rights and liberties, ethics, and risk management in the context of AI.[35]

B. BLUEPRINT FOR AN AI BILL OF RIGHTS: MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE

AI has been met with a growing public concern for the protection of individual rights and privacy across the globe. In response, the White House Office of Science and Technology Policy ("OSTP") released the AI Bill of Rights.[36] Established in 1976, OSTP is committed to using science and technology to improve health, prosperity, security, environmental quality, and justice for all Americans.[37] OSTP is made up of six teams, including a technology team committed to "advance[ing] technology and data to benefit all Americans."[38]

Although the AI Bill of Rights is not a law and does not create legal rights,[39] it aims to replicate the influence of the RCRC and FIPPs by providing industries with "principles that should guide the design, use, and deployment of automated systems."[40] In addition to providing guidance for the design, use, and deployment of automated systems, the AI Bill of Rights also uses specific language to prevent companies from evading its principles. The AI Bill of Rights notably never refers to algorithms or artificial intelligence.[41] Instead, it refers to "automated systems," which are defined

---

34 AI BILL OF RIGHTS, *supra* note 6, at 9.

35 *Id.* at 9.

36 *Id.* at 3.

37 *Office of Science and Technology Policy*, THE WHITE HOUSE, https://www.whitehouse.gov/ostp/ [https://perma.cc/8KQ9-X3PM] (last visited: Feb. 13, 2023).

38 *OSTP's Teams: Technology*, THE WHITE HOUSE, https://www.whitehouse.gov/ostp/ostps-teams/technology/ [https://perma.cc/TX4L-8UHN] (last visited Jan. 4, 2023).

39 *See* AI BILL OF RIGHTS, *supra* note 6, at 2 ("The *Blueprint for an AI Bill of Rights* is not intended to, and does not, create any legal right, benefit, or defense, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person, nor does it constitute a waiver of sovereign immunity.").

40 *Id.* at 3.

41 *See* Peter J. Schildkraut, James W. Kim, Marne Marotta, James V. Courtney, Jr. & Paul J. Waters, *The "Blueprint for an AI Bill of Rights"*, ARNOLD & PORTER (Oct. 27, 2022), https://www.arnoldporter.com/en/perspectives/advisories/2022/10/the-blueprint-for-an-ai-

as "includ[ing], but [is] not limited to, systems derived from machine learning, statistics, or other data processing or artificial intelligence techniques, and exclude passive computing infrastructure."[42] The automated systems language aims to act as a catch all umbrella and prevent companies from naming around the issue.[43]

The AI Bill of Right's five principles are as follows: Safe and Effective Systems ("Safety"); Algorithmic Discrimination Protections ("Algorithmic Discrimination"); Data Privacy, Notice and Explanation ("Notice"); and Human Alternatives, Consideration, and Fallback ("Human Alternatives").[44]

First, the Safety principle aims to ensure that all individuals subject to automated systems have a fair and equitable experience.[45] It mandates that automated systems must undergo pre-deployment testing, risk identification and mitigation, and ongoing monitoring to ensure their safety and effectiveness.[46]

In 2019, major platforms, such as Facebook, YouTube, and Twitter, turned to automated systems to curb the spread of hateful speech on their platforms.[47] However, the use of automated systems had a discriminatory effect and silenced the speech of Black people using African American Vernacular English ("AAVE").[48] Similarly, TikTok's use of a recommendation algorithm to sort its users' content feed resulted in the

---

bill-of-rights [https://perma.cc/A2E2-KZAK] ("In the debate over the EU's pending Artificial Intelligence Act, the definition of 'artificial intelligence' has attracted much discussion. OSTP sidesteps this issue in the blueprint by addressing 'automated systems,' which are defined as 'any system, software or process that uses computation as whole or part of a system to determine outcomes, make or aid decisions, inform policy implementation, collect data or observations, or otherwise interact with individuals and/or communities.'").

42 AI BILL OF RIGHTS, *supra* note 6, at 10.

43 *See* Daniel Bashir, *Suresh Venkatasubramanian: An AI Bill of Rights*, THE GRADIENT, at 54:20 (Jan. 12, 2023), https://thegradientpub.substack.com/p/suresh-venkatasubramanian-an-ai-bill#details (advocating against legislation using the term "artificial intelligence").

44 AI BILL OF RIGHTS, *supra* note 6, at 5–7.

45 *See* AI BILL OF RIGHTS, *supra* note 6, at 5 ("Automated systems should be developed with consultation from diverse communities, stakeholders, and domain experts to identify concerns, risks, and potential impacts of the system.").

46 *Id.*

47 Shirin Ghaffary, *How TikTok's Hate Speech Detection Tool Set Off a Debate About Racial Bias on the App*, VOX (July 7, 2021, 8:24 PM), https://www.vox.com/recode/2021/7/7/22566017/tiktok-black-creators-ziggi-tyler-debate-about-black-lives-matter-racial-bias-social-media [https://perma.cc/T3H7-WCB5].

48 *See id.* ("[A] study showed that leading AI models for detecting hate speech are 1.5 times more likely to flag tweets written by African Americans as 'offensive' compared to other tweets.").

suppression of creators of colors's content.[49] The Safety principle would have addressed this issue by including diverse community stakeholders in the development of the automated system to avoid the voices of Black people being silenced.

Second, the Algorithmic Discrimination principle aims to draw attention to the issue of discriminatory outcomes and places the responsibility on developers and deployers to take proactive measures to prevent such discrimination in their automated systems.[50] In 2018, Joy Buolamwini, an MIT Media Lab researcher, discovered that facial detection algorithms failed to detect dark-skinned faces.[51] The algorithm discriminated against individuals with darker complexions due to a lack of dark-skinned facial training data.[52] The Algorithmic Discrimination principle aims to address this issue by ensuring that developers and deployers take active steps to mitigate it before deployment.

Third, the Data Privacy principle aims to ensure that only necessary and critical data is collected.[53] For example, a bank may use data in its automated system to determine whether or not to grant an individual a loan.[54] Conversely, a social media platform utilizing a recommendation algorithm to sort content on a user's feed does not require this sensitive user information

---

49 *See* Amarikwa, *supra* note 11, at 128 ("BookTok presents a clearer example of how the recommendation algorithm compounds and expands an industry's existing racial inequalities . . . Black creators have suggested that authors of color are excluded from BookTok because the TikTok algorithm prioritizes White creators' content.").

50 *See* AI BILL OF RIGHTS, *supra* note 6, at 5 ("Algorithmic discrimination occurs when automated systems contribute to unjustified different treatment or impacts disfavoring people based on their race, color, ethnicity, sex (including pregnancy, childbirth, and related medical conditions, gender identity, intersex status, and sexual orientation), religion, age, national origin, disability, veteran status, genetic information, or any other classification protected by law.").

51 Joy Buolamwini, *When the Robot Doesn't See Dark Skin*, N.Y. TIMES (June 21, 2018), https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html.

52 *See id.* ("So if more white males with generally homogeneous mannerisms have been hired in the past, it's possible that algorithms will be trained to favorably rate predominantly fair-skinned, male candidates while penalizing women and people of color who do not exhibit the same verbal and nonverbal cues").

53 *See* AI BILL OF RIGHTS, *supra* note 6, at 6 ("You should be protected from violations of privacy through design choices that ensure such protections are included by default, including ensuring that data collection conforms to reasonable expectations and that only data strictly necessary for the specific context is collected.").

54 *See* Sian Townson, *AI Can Make Bank Loans More Fair*, HARV. BUS. REV. (Nov. 6, 2020), https://hbr.org/2020/11/ai-can-make-bank-loans-more-fair [https://perma.cc/S4JA-BBZN] (describing how the use of demographic data, such as gender and ethnicity may result in biased AI outcomes).

to operate.[55] Thus, the Data Privacy principle, similar to the RCRC,[56] seeks to limit the use of users' data and shift control from deployers and developers to users.

Fourth, the Notice principle aims to encourage deployers to provide plain-text information regarding the operation of the automated systems to individuals.[57] Although platforms may provide some background on how their algorithms work, the working of the algorithm remains largely opaque.[58] For example, certain generative AI models like Llama 2 share their training data,[59] whereas most other industry leaders provide broad overviews at best.[60] The Notice principle aims to notify people that algorithms are being used and how these algorithms make decisions.

Finally, the Human Alternatives principle provides an avenue for recourse and redress for individuals subject to automated systems.[61] It offers individuals the choice to opt-out in favor of a human decision maker and allows users to challenge automated systems' decisions if they find them to be erroneous.[62] While some commentators argue that algorithms involve less

---

55 *See* Amarikwa, *supra* note 11, at 128 (describing how TikTok's recommendation algorithm works and collects user data).

56 *See* U.S. DEP'T OF HEALTH, EDUC., & WELFARE, *supra* note 15, at xx (describing how users should be able to consent to data uses).

57 *See* AI BILL OF RIGHTS, *supra* note 6, at 6 ("Designers, developers, and deployers of automated systems should provide generally accessible plain language documentation including clear descriptions of the overall system functioning and the role automation plays, notice that such systems are in use, the individual or organization responsible for the system, and explanations of outcomes that are clear, timely, and accessible.").

58 *See, e.g.*, Kartik Hosanagar & Vivian Jair, *We Need Transparency in Algorithms, but Too Much Can Backfire*, HARV. BUS. REV. (July 23, 2018), https://hbr.org/2018/07/we-need-transparency-in-algorithms-but-too-much-can-backfire [https://perma.cc/A66J-A5SZ] ("[S]ome of today's best-performing algorithms are often the most opaque."); *see also* Electronic Privacy Information Center, Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem 76 (Nov. 2022) ("Educational institutions are increasingly using opaque algorithms to generate predictions about students and according differential treatment based on those predictions.").

59 *See* Hugo Touvron et al., *Llama 2: Open Foundation and Fine-Tuned Chat Models* 4 (Jul. 19, 2023) (manuscript), https://arxiv.org/pdf/2307.09288.pdf [https://perma.cc/T5QA-V9VW] (discussing the model's training process).

60 *See* Melissa Heikkilä, *OpenAI's Hunger for Data is Coming Back to Bite It*, MASS. INST. TECH. TECH. REV. (Apr. 19, 2023), https://www.technologyreview.com/2023/04/19/1071789/openais-hunger-for-data-is-coming-back-to-bite-it/ [https://perma.cc/4H7N-KFA2] (highlighting how even tech companies often have a limited understanding of their algorithms' training data).

61 *See* AI BILL OF RIGHTS, *supra* note 6, at 7 ("You should be able to opt out from automated systems in favor of a human alternative, where appropriate.").

62 *See id.*6 ("You should be able to opt out from automated systems in favor of a human alternative, where appropriate.").

bias than human decision makers,[63] there is still a growing distrust of algorithmic decision-making.[64] Therefore, the Human Alternatives principle seeks to provide people with an alternative option, thereby giving individuals greater control over the decisions that affect their lives.

The main critic of the AI Bill of Rights is that it is toothless and does little to regulate the use of automated systems.[65] Critics argue that it does not go far enough in its enforcement efforts and is a "is an insult to both AI and the Bill of Rights."[66] However, the AI Bill of Rights itself notes that it does not aim to provide any legal rights.[67] Rather it intends to serve an advisory role similar to the FIPPs.[68]

---

63 Alex P. Miller, *Want Less-Biased Decisions? Use Algorithms*, HARV. BUS. REV. (July 26, 2018), https://hbr.org/2018/07/want-less-biased-decisions-use-algorithms [https://perma.cc/73CZ-883R].

64 Cade Massey & Joseph Simmons, *Why Humans Distrust Algorithms – and How That Can Change*, KNOWLEDGE AT WHARTON (Feb. 13, 2017), https://knowledge.wharton.upenn.edu/article/how-to-convince-people-to-trust-algorithms/ [https://perma.cc/HKE6-UY39].

65 *See, e.g.*, Alex Engler, *The AI Bill of Rights Makes Uneven Progress on Algorithmic Protections*, BROOKINGS (Nov. 21, 2022), https://www.brookings.edu/2022/11/21/the-ai-bill-of-rights-makes-uneven-progress-on-algorithmic-protections/ [https://perma.cc/4G75-F4L3] ("But, because they are nonbinding, the degree to which the AIBoR will culminate in substantial changes to these systems is largely dependent on the actions of federal agencies."); *see also* Makenzie Holland, *AI Bill of Rights Blueprint Lacks Enforceability*, TECHTARGET (Oct. 4, 2022), https://www.techtarget.com/searchenterpriseai/news/252525704/AI-bill-of-rights-blueprint-lacks-enforceability [https://perma.cc/3TTM-WGU5] ("The main problem with the AI Bill of Rights is it has no teeth, said Alan Pelz-Sharpe, founder of market analysis firm Deep Analysis."); *see also* Khari Johnson, *Biden's AI Bill of Rights Is Toothless Against Big Tech*, WIRED (Oct. 4, 2022), https://www.wired.com/story/bidens-ai-bill-of-rights-is-toothless-against-big-tech/ [https://perma.cc/MM7L-MWPV] ("However, unlike the better known US Bill of Rights, which comprises the first 10 amendments to the constitution, the AI version will not have the force of law—it's a nonbinding white paper.").

66 Daniel Castro, *White House AI Bill of Rights Is All Wrong, Says Center for Data Innovation*, CTR. FOR DATA INNOVATION (Oct. 5, 2022), https://datainnovation.org/2022/10/white-house-ai-bill-of-rights-is-all-wrong-says-center-for-data-innovation/ [https://perma.cc/2U63-BDLQ]; *see* CNTR. FOR EUR. PERSP., STRATEGIC P'SHIP FOR A SECURE AND DIGIT. EUROPE 31 (Nov. 2022) ("[T]he 'plan lacks teeth' and the US needs even tougher regulation around AI."); *see also* Michael Capps, *Coming AI Regulation May Not Protect Us from Dangerous AI*, VENTURE BEAT (Feb. 4, 2023), https://venturebeat.com/ai/coming-ai-regulation-may-not-protect-us-from-dangerous-ai/ ("Neither framework demands enough transparency from AI systems. Neither framework provides enough protection for the public or enough regulation for business. A series of analyses provided to the EU have pointed out the flaws in the AI Act.").

67 AI BILL OF RIGHTS, *supra* note 6, at 2.

68 *Id.* at 9.

Others argue that the AI Bill of Rights focuses on consumers fails to adequately take workers into consideration.[69] For example, Facebook relies on automated systems to detect harmful content, but with the Human Alternatives principle, users may choose to opt-out of the automated review in favor of human oversight.[70] The result of this policy is to require humans instead of algorithms to review content, which has detrimental impacts on moderators' wellbeing.[71] Platforms like OpenAI and TikTok, which rely on human review to detect harmful content, have faced criticism for their poor treatment of workers and the impact it has on their mental health.[72] Human review requires workers, typically working in the global south, to be regularly exposed to harmful and abusive content.[73] The principles protect consumers and users at the expense of workers as they're exposed to greater harms.

In conclusion, while the AI Bill of Rights has faced criticism for its enforcement efforts and lack of consideration for workers, it is important to recognize its intended advisory role. The AI Bill of Rights can guide industries in the design, use, and deployment of automated systems in the

---

69 *See* Stephen Ritter, *It's Time to Look Harder at the Morality of AI*, FORBES (Jan. 25, 2023), https://www.forbes.com/sites/forbestechcouncil/2023/01/25/its-time-to-look-harder-at-the-morality-of-ai/?sh=29a544c8522e [https://perma.cc/VH48-FVDX] ("I question whether we are giving adequate thought to—and building sufficient guardrails around—AI's impact on the world's workers.").

70 *See* Tom Simonite, *Facebook Is Everywhere; Its Moderation Is Nowhere Close*, WIRED (Oct. 25, 2021), https://www.wired.com/story/facebooks-global-reach-exceeds-linguistic-grasp/#:~:text=Facebook%20says%20it%20has%20automated,to%20solve%20the%20company%27s%20problems ("Facebook says it has automated systems to find hate speech and terrorism content in more than 50 languages.").

71 *See* Andrew Arsht & Daniel Etcovitch, *The Human Cost of Online Content Moderation*, HARV. JOLT DIGEST (Mar. 2, 2018), https://jolt.law.harvard.edu/digest/the-human-cost-of-online-content-moderation [https://perma.cc/XE2M-S6WR] ("Who enforces the content guidelines promulgated by mega-platforms that host user-generated content, such as Facebook, Twitter, and YouTube? While the specifics remain intentionally obfuscated, content moderation is done by tens of thousands of online content moderators . . . there is a growing body of evidence that content moderation, as currently constituted, entails considerable psychological risks to the employee.").

72 *See, e.g.*, Rosie Bradbury & Majd Al-Waheidi, *A Factory Line of Terrors: TikTok's African Content Moderators Complain They Were Treated Like Robots, Reviewing Videos of Suicide and Animal Cruelty for Less Than $3 an Hour.*, BUS. INSIDER (Aug. 1, 2022), https://www.businessinsider.com/tiktoks-african-factory-line-of-terrors-2022-7 [https://perma.cc/4QKM-5EMK] ("Nine current and former content moderators in Morocco . . . described experiences of severe psychological distress as a result of their jobs."); *see also* Billy Perrigo, *Exclusive: OpenAI Used Kenyan Workers on Less than $2 per Hour to Make ChatGPT Less Toxic*, TIME (Jan. 18, 2023), https://time.com/6247678/openai-chatgpt-kenya-workers/ [https://perma.cc/QG4H-VXZ9] (describing how ChatGPT outsourced the work of reviewing graphic violent content for open AI learning to a firm in Kenya).

73 *Id.*

US. As with the FIPPs, the AI Bill of Rights has the potential to shape the future of regulation, and it is crucial to scrutinize and address any potential constitutional issues that may emerge from its adoption.

II. CONSTITUTIONAL CHALLENGES

As AI becomes increasingly integrated into our daily lives, concerns around accountability and transparency have arisen. To address these concerns, the AI Bill of Rights was created, outlining a set of principles that aim to ensure ethical and responsible use of AI. However, as with any proposed legislation, potential legal challenges must be considered. In particular, the AI Bill of Rights' Notice principle, which requires automated systems to provide explanations and documentation for their decisions, may conflict with the First Amendment's free speech protections. Additionally, the adoption of the Data Privacy and Human Alternatives principles may also pose Fifth Amendment Takings Clause issues. This Part explores these legal considerations and potential solutions to ensure that laws adopting the AI Bill of Right's principles effectively promote accountability and transparency while upholding private rights.

A. FIRST AMENDMENT

The regulation of algorithmic speech has raised important legal questions about the First Amendment's Compelled Speech Doctrine, which prohibits the government from forcing individuals to express or support views they disagree with. Although the Supreme Court has not provided clear guidance on the protection of algorithmic speech under the First Amendment, courts generally agree that some forms of algorithmic speech deserve constitutional protections. However, regulating algorithmic speech using the AI Bill of Rights principles could face challenges due to the Notice principle's documentation and outcome explanations requirements.

This Section is structured into four parts to examine the issue of regulating algorithmic speech. First, I present an overview of the First Amendment and the Compelled Speech Doctrine. Second, various scholars' interpretations of how the courts will address the issue of algorithmic speech under the First Amendment are examined. Third, an overview of district court cases that specifically address the regulation of private companies employing algorithms is given. Finally, the Section will conclude by

discussing the potential constitutional violations that the AI Bill of Right's Notice principles may face if lawmakers choose to adopt them. The AI Bill of Rights' Notice principle, designed to promote accountability and transparency in automated systems, faces potential constitutional challenges, particularly regarding the First Amendment's free speech protections.

1. Compelled Speech Doctrine

The First Amendment's Compelled Speech Doctrine protects individuals' choice to speak and not to speak. This doctrine has been shaped by several Supreme Court cases, including *Barnette*, *Tornillo*, *Maynard*, and *Janus*, which established the principle that the government cannot force individuals to support views they disagree with. The emergence of new technologies and algorithmic speech has raised novel legal questions about the application of the Compelled Speech Doctrine. This Section provides an overview of the Compelled Speech Doctrine before exploring the application of the Doctrine to emerging technologies in the subsequent sections.

The First Amendment of the U.S. Constitution prohibits Congress from passing laws that limit the exercise of free speech or freedom of the press.[74] The Supreme Court has interpreted the term "speech" broadly and recognized that the creation of information is also considered "speech" under the First Amendment.[75]

The First Amendment's Compelled Speech Doctrine holds that individuals have the choice to speak and not to speak.[76] This is reflected in a series of Supreme Court holdings. In *Barnette*, the Court held that schools could not force children to recite the Pledge of Allegiance nor salute the

---

74 U.S. CONST. amend. I.

75 *See* Bartnicki v. Vopper, 532 U.S. 514, 527 (2001) ("[I]f the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct."); *see also* Rumsfeld v. F. for Acad. & Inst. Rts., Inc., 547 U.S. 47, 61 (2006) ("[F]reedom of speech prohibits the government from telling people what they must say."); *see also* Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS. L. REV. 1149, 1159 (2018) ("Information is speech, and speech is protected by the First Amendment.").

76 *See* Eugene Volokh, *The Law of Compelled Speech*, 97 TEX. L. REV. 355, 355 (2018) (citing Riley v. Nat'l Fed'n of the Blind of N.C., Inc., 487 U.S. 781, 796–97 (1988)) ("Speech compulsions, the Court has often held, are as constitutionally suspect as are speech restrictions: '[T]he First Amendment guarantees 'freedom of speech,' a term necessarily comprising the decision of both what to say and what not to say.'").

flag.[77] In *Tornillo*, the Court held that Florida could not require newspapers to publish the replies of political candidates.[78] In *Maynard*, the Court held that New Hampshire could not require drivers to display the government approved message on their license plates.[79] In *Janus*, the Court held that the government cannot force individuals to "mouth support" for political views they disagree with by mandating union dues that fund political speech.[80]

In summary, the First Amendment's Compelled Speech Doctrine protects individuals' choice to speak and not to speak and has been shaped by several Supreme Court cases. With the emergence of automated systems, it raises the question, is algorithmic speech protected under the First Amendment?

2. Perspectives from Legal Scholars: the First Amendment and Algorithmic Speech

The regulation of algorithms has become a complex legal issue in recent years, with scholars debating whether algorithmic speech should be protected under the First Amendment. Although there is a general consensus among legal scholars that some forms of algorithmic speech may be protected under the First Amendment, the scope of protection is a contentious issue. Additionally, legal scholars hold varying opinions on how the Court will rule regarding transparency requirements. This Section explores the perspectives of various legal scholars on the relationship between algorithmic speech and the First Amendment.

Jennifer K. Wagner, an assistant professor of law and engineering at Penn State Law, contends that the regulation of algorithms may pose challenges due to potential conflicts with the Compelled Speech Doctrine.[81] According to Wagner, it is an open question as to whether mandates for privacy-by-design practices may be considered "compelled silence," and whether mandated non-discrimination-by-design principles may be viewed as

---

77 W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 642 (1943).

78 Miami Herald Publishing Company v. Tornillo, 418 U.S. 241, 258 (1974).

79 Wooley v. Maynard, 430 U.S. 705, 707 (1977).

80 Janus v. AFSCME, 138 S. Ct. 2448, 2463 (2018).

81 *See* Jennifer K. Wagner, *Algorithmic Fairness in the Roberts Court Era*, PACIFIC SYMP. ON BIOCOMPUTING 519, 526 (2023) ("[G]overnment-imposed data practice rules (e.g., regarding collection, management, processing, and disclosures) to promote algorithmic fairness and equal participation in, access to, and shared benefits and burdens of digital health and biomedical data science are going to be extremely difficult to realize in the Roberts Court era.").

"compelled speech" rather than mandated conduct.[82] This raises concerns that regulations promoting algorithmic fairness and addressing data biases may be considered content-based compelled speech, making it difficult to impose government regulations.[83]

To bypass the First Amendment limitations on regulating algorithms, legal scholars have proposed privacy and antitrust regulations as more viable options.[84] However, such regulations might face resistance from platforms due to their potential impact on business models.[85]

Jack M. Balkin, a constitutional law professor at Yale Law School, finds that the most important question is whether companies will be able to shield themselves from regulation by claiming that their uses of AI agents, robots, and algorithms are First Amendment protected activities.[86] He notes that the First Amendment could be exploited by companies to justify their surveillance and control over populations, making existing First Amendment doctrines inadequate to protect free expression.[87] Similarly, Ash Carter and Amritha Jayanti, directors at the Harvard Kennedy School's Belfer Center, argue that social media content recommendation algorithms may be protected under the First Amendment.[88]

To get around the First Amendment concerns, Balkin introduces the concepts of information fiduciaries to clarify when the state can regulate companies that collect, analyze, and distribute data under the First Amendment.[89] Information fiduciaries collect sensitive information with the consent of their clients and have a fiduciary duty to protect that information, although this duty may have less stringent obligations compared to those of

---

82 Wagner, *supra* note 82, at 525.

83 Wagner's view is echoed by Justice Kavanaugh. *See* Am. Meat Inst. v. United States Dep't of Agric., 760 F.3d 18, 33 (2014) (J. Kavanaugh, concurring) ("It is important to underscore that those *Zauderer* fit requirements are far more stringent than mere rational basis review. When the Supreme Court applies rational basis review, it does not attach a host of requirements of the kind prescribed by *Zauderer*."); Wagner, *supra* note 82, at 525.

84 Ash Carter & Amritha Jayanti, *Technology Primers for Policymakers: Social Media Recommendation Algorithms*, BELFER CTR. at 21–22 (Aug. 2022).

85 *See id.* at 22 (e.g., compliance with the California Consumer Privacy Act (CCPA) requires social media companies to allow users to delete their personal information from the recommendation algorithm).

86 Balkin, *supra* note 76, at 1159.

87 *Id.*

88 *See* Carter & Jayanti, *supra* note 85, at 20–21.

89 *See* Balkin, *supra* note 76, at 1154–65.

traditional professionals.[90] Balkin concludes that similar to how the First Amendment does not prevent the state from regulating how professionals interact with their clients, governments can subject an information fiduciary to reasonable restrictions on data processing of personal information.[91]

Stuart Minor Benjamin, a law professor at Duke University School of Law, explores the question of what activities are protected under the First Amendment in the context of algorithmic decision making.[92] Benjamin argues that algorithms do not convert speech into non-speech.[93] Thus, incorporating algorithmic decision-making within the purview of the First Amendment is a reasonable and logical step if humans are making substantive editorial decisions and communication is not eliminated.[94]

Addressing the issue of transparency requirements, Eric Goldman, an internet law professor at Santa Clara University School of Law, argues that mandatory editorial transparency conflicts with the First Amendment.[95] He cites *Lando*, which held that the editorial process is not subject to examination to serve a general public interest.[96] Specifically, looking at *NetChoice v. Paxton*,[97] Goldman finds that social media platforms "qualify for the same constitutional protections as traditional publishers" and mandatory editorial transparency requires strict scrutiny.[98] Goldman argues that under strict scrutiny, mandatory editorial transparency laws are likely to fail constitutional challenges because they often fail to achieve their intended goals.[99]

---

90 Balkin, *supra* note 76, at 1162–63.

91 Balkin, *supra* note 76, at 1162.

92 Stuart Minor Benjamin, *Algorithms and Speech*, 161 U. PA. L. REV. 1145 (2013).

93 *See* Benjamin, *supra* note 93, at 1471 ("Nothing in the Court's jurisprudence supports the proposition that reliance on algorithms transforms speech into nonspeech.").

94 Benjamin, *supra* note 92, at 1494.

95 *See* Eric Goldman, *The Constitutionality of Mandating Editorial Transparency*, 73 HASTING L. J. 1203 (2022).

96 *See* Goldman, *supra* note 96, at 1215 (citing Herbert v. Lando, 441 U.S. 153, 174 (1979)) ("The Herbert majority added this crucial qualification: '[t]here is no law that subjects the editorial process to private or official examination merely to satisfy curiosity or to serve some general end such as the public interest; and if there were, it would not survive constitutional scrutiny as the First Amendment is presently construed.'")

97 *See* NetChoice, LLC v. Paxton, 49 F.4th 439 (5th Cir. 2022) (challenging a Texas law that would require social media platforms to host third-party content and produce biannual transparency reports).

98 Goldman, *supra* note 96, at 1224.

99 Goldman, *supra* note 96, at 1217.

In conclusion, while legal scholars generally agree that algorithmic speech may be protected under the First Amendment, the extent of protection and the application of the Compelled Speech Doctrine to automated systems remains a contentious issue.

3. Cases on the Regulation of Algorithmic Decision-Making by Private Companies

The Supreme Court's silence on the issue has led to a circuit split. In this Section, I will examine various court decisions related to the Compelled Speech Doctrine and their implications for the regulation of algorithms.

In *Zauderer*, the Supreme Court held that the government may compel private speech as long as the speech is "purely factual and uncontroversial."[100] Under the *Zauderer* standard, the commercial disclosure requirement must be "reasonably related to the State's interest in preventing deception of consumers" and must not be "[u]njustified or unduly burdensome" such that it would "chill[] protected speech."[101] The Court reasoned that purely factual information implicates minimal intrusion on the speaker's First Amendment rights.[102]

The Fifth Circuit expanded on this view in *Arnold*, holding that the government may defeat a compelled speech claim if it can show that it is an "essential [government] operation[]," required for the preservation of an orderly society.[103] Conversely, the Second Circuit held that the government could not defeat a compelled speech claim because the First Amendment right not to speak protects the right to refuse to make false statements to the government.[104]

In recent years, the constitutionality of state laws that seek to regulate the use of algorithms by private companies has become a prominent issue before the courts. Notably, the Eleventh and Fifth Circuit have addressed specific issues related to these regulations and have reached differing conclusions, highlighting the complex nature of these legal questions.

---

100 Zauderer v. Off. of Disciplinary Couns. of Sup. Ct., 471 U.S. 626, 651(1985).

101 NetChoice, LLC v. AG Fla., 34 F.4th 1196, at 1230 (11th Cir. 2022) (citing Milavetz, Gallop & Milavetz, P.A. v. United States, 559 U.S. 229, 250 (2010)).

102 471 U.S. at 651.

103 United States v. Arnold, 740 F.3d 1032, 1035 (5th Cir. 2014) (quoting United States v. Sindel, 53 F.3d 874, 878 (8th Cir. 1995)) (internal quotations omitted).

104 Burns v. Martuscello, 890 F.3d 77, 86 (2d Cir. 2018) (citing Jackler v. Byrne, 658 F.3d 225, 241 (2d Cir. 2011)).

The Eleventh Circuit relied on *Zauderer* in a case involving a Florida statute including disclosure provisions, which required platforms to provide a "thorough rationale" for each and every content-moderation decision they made.[105] The court held that the disclosure provision was unconstitutional under *Zauderer* because it was unduly burdensome and likely to chill protected speech.[106]

Conversely, the Fifth Circuit addressed the compelled speech issue differently in *NetChoice v. Paxton*. In this case, the plaintiffs alleged that a Texas law requiring transparency reports violated the First Amendment.[107] The transparency reports required the platform to publish a report containing statistics about their content-moderation activities every six months.[108] The Fifth Circuit found that the First Amendment had not been violated, because the platforms failed to demonstrate how tracking metrics may "unduly burden [their] protected *speech*."[109]

In conclusion, the Compelled Speech Doctrine, and its application to automated systems, has resulted in a circuit split due to the absence of a clear standard. While the *Zauderer* standard provides some guidance, courts have varied in their interpretations of its scope and applicability.

4. First Amendment Considerations for the AI Bill of Rights

The AI Bill of Rights principles are subject to various legal considerations, with the Notice principle being particularly vulnerable to First Amendment issues. The Notice principle aims to ensure accountability of those in control of automated systems by making the public aware of their functionality and usage.[110] This Section explores the constitutionality of regulations that require private companies to comply with the Notice principle's document disclosures and outcome regulations.

Automated systems have increasingly become a part of decision-making processes, raising concerns about transparency and accountability. To

---

105 NetChoice, LLC v. Att'y Gen., Florida 34 F.4th 1196, 1223, 1230 (11th Cir. 2022).

106 *Id.* at 1230.

107 *See Association Members*, NETCHOICE, https://netchoice.org/about/#association-members [https://perma.cc/RA75-46GV] (last visited: Mar. 25, 2023) (including associational members such as Google, TikTok, Twitter, and Meta).

108 NetChoice, LLC v. Paxton, 49 F.4th at 485.

109 *Id.* at 486.

110 AI BILL OF RIGHTS, *supra* note 6, at 6.

address this, the AI Bill of Right's Notice principle was developed to ensure that those in control of automated systems are held accountable by putting the public on notice about their functionality and usage.[111] The Notice principle includes four main provisions, publishing documentation about system functionality, reporting system usage, listing system owners, and explaining the system's outcomes.[112]

The outcome explanation requirement, which requires that users be made aware of how and why an automated system determined an outcome impacting them, more likely violates the Compelled Speech Doctrine. Unlike the documentation requirement, this requirement would require automated systems to provide explanations for millions of decisions. For example, TikTok's recommendation algorithm uses various factors to create a personalized feed for each user, making it difficult to explain why a specific video was recommended to a particular user.[113] As such, the outcome explanation requirement may be deemed unduly burdensome, similar to the Florida disclosure requirement that was enjoined in *NetChoice v. Attorney General, Florida*.

One case in which this principle might apply is when an individual submits a job application and the employer uses an algorithm to screen resumes.[114] The AI Bill of Rights states that the applicant should "know how and why an outcome impacting you was determined by an automated system, including when the automated system is not the sole input determining the outcome." In such a case, the Notice principle would require the employer to make applicants aware that automated systems were being used to review their resume.[115] This presents issues as allowing applicants to understand how outcomes are determined may allow applicants to game the system, thereby defeating the purpose of the algorithmic evaluation. Citing *Sorrell v. IMS Health System*, scholars have noted that transparency and notice

111 AI BILL OF RIGHTS, *supra* note 6, at 6.

112 AI BILL OF RIGHTS, *supra* note 6, at 40.

113 *See* Amarikwa, *supra* note 11, at 82; *How TikTok Recommends Videos #ForYou*, TIKTOK (June 18, 2020), https://newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you [https://perma.cc/2WH2-EMN6].

114 Ifeoma Ajunwa, *Beware of Automated Hiring*, N.Y. TIMES (Oct. 8, 2019), https://www.nytimes.com/2019/10/08/opinion/ai-hiring-discrimination.html [https://perma.cc/EZ65-T28M] ("Employers are increasingly using [algorithms] during the hiring process out of the belief they're both more convenient and less biased than humans.").

115 AI BILL OF RIGHTS, *supra* note 6, at 40.

requirements for systems may be seen as coerced speech.[116] This may also implicate a Takings violation if the regulation renders the algorithm useless or incapable of extracting value.

Lawmakers seeking to incorporate the Notice principle into future laws should exercise caution. The Notice principle includes four main provisions: publishing documentation about system functionality, reporting system usage, listing system owners, and explaining the system's outcomes. Reporting system usage and listing system owners are in line with transparency requirements outlined in the FIPPs, and therefore are generally considered acceptable provisions of the Notice principle.

The main issues arise with the adoption of the documentation and outcomes explanation requirements. Their acceptability depends on how demanding the laws are. For example, the Fifth Circuit upheld the documentation requirement in *Paxton*, which required online platforms to release a biannual report containing high-level statistics related to the content moderation efforts platforms.[117] However, the Eleventh Circuit found the documentation and outcomes explanation requirement required by Florida statute to be "unduly burdensome," because it required platforms to explain countless decisions.[118]

Legislators seeking to require platforms to provide high-level documentation of their automated system's functionality are unlikely to violate the First Amendment. However, if the regulation mandates detailed descriptions of how the system works, it could potentially be viewed as a violation of the First Amendment. Similarly, requiring detailed explanations of system outcomes is also likely to be seen as unduly burdensome and a violation of the First Amendment. Ultimately, whether the documentation and outcomes requirement violates the Compelled Speech Doctrine may depend on whether it is reasonably related to preventing consumer deception

---

116 *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 21 (2014) ("Given the Supreme Court's ruling in *Sorrell v. IMS Health Inc.* and other rulings in cases involving the regulation of ranking systems, courts may look askance at rules that limit the dissemination of data or scores. Nevertheless, scored individuals should be notified when scores or data are communicated to an entity. That notification only *increases* speech; it does not restrict or censor communication. Coerced speech can implicate the First Amendment, but like Professor Neil Richards, we do not understand *Sorrell* to lay down a blanket rule that all data is speech.")

117 *See* 49 F.4th at 486.

118 *See* 34 F.4th at 1230.

and whether platforms already provide such information, making it less burdensome.

In conclusion, while the Notice principle aims to address issues of transparency and accountability in automated decision-making processes, its requirements may need to be reexamined to ensure that they do not unduly burden automated system owners and violate the First Amendment.

B. FIFTH AMENDMENT

The Takings Clause of the Fifth Amendment was initially applied to the physical taking of private property by the government, but it has since been expanded to include intangible assets and regulatory takings. Recently, the application of the Takings Clause to online platforms and automated systems has become a significant topic of interest and concern.

This Section is structured in four parts to examine the issue of applying the Takings Clause to automated systems regulation. First, a comprehensive overview of the Takings Clause will be provided. Second, the split among courts applying the Takings Clause to automated systems regulation will be explained. Third, the ongoing debate among scholars relating to the Takings Clause and automated systems will be briefly discussed. Finally, I will examine how the principles of the AI Bill of Rights, specifically the Data Privacy and Human Alternatives principles, may trigger the Takings Clause. The adoption of the AI Bill of Rights' Data Privacy and Human Alternatives principles may conflict with the Fifth Amendment's Takings Clause if it results in regulatory takings that significantly curtail private parties' ability to utilize their intangible property.

1. Takings Clause

The Takings Clause of the Fifth Amendment states "[n]or shall private property be taken for public use, without just compensation."[119] The Supreme Court has interpreted the Takings Clause as requiring compensation for the taking of all forms of private property,[120] including

---

119 US CONST. amend. V.

120 Richard A. Epstein & Eduardo M. Peñalver, *The Fifth Amendment Takings Clause*, CONST. CTR., https://constitutioncenter.org/the-constitution/amendments/amendment-v/clauses/634 [https://perma.cc/7S4S-73AJ] (last visited Apr. 2, 2023).

intangible assets like intellectual property.[121] The Court's ruling in *Pennsylvania Coal v. Mahon* expanded the scope of the Takings Clause to include situations where "government regulation 'goes too far' in diminishing the value of private property."[122] However, the Court has also acknowledged that regulations aimed at promoting the common good are generally accepted and not considered to be regulatory takings.[123]

In summary, the Takings Clause of the Fifth Amendment has evolved over time to apply to various types of takings including the taking of intangible assets and regulatory takings. As technology continues to advance, the application of the Takings Clause to digital platforms and automated systems has become increasingly complex. The principles of the AI Bill of Rights further complicate the issue by raising questions about the economic value of digital assets and the impact of regulations on their value.

2. Cases on Regulatory Takings

When it comes to regulating these systems, it is essential to consider how economic issues factor into the analysis. One case that highlights this issue is *Armstrong v. United States*, where the Supreme Court held that because the government's actions destroyed the value of the petitioner's liens, a takings occurred and the petitioners were entitled to compensation.[124] The Court stated that:

> The total destruction by the Government of all value of these liens, which constitute compensable property, has every possible element of a Fifth Amendment "taking" and is not a mere "consequential incidence" of a valid regulatory measure. Before the liens were destroyed, the lienholders admittedly had compensable property. Immediately afterwards, they had none. This was not because their property vanished into thin air. It was because the Government for its own advantage destroyed the value of the liens. . . .[125]

However, it remains unclear how courts will address the issue of whether requiring technology companies to comply with regulations that alter the management of their platforms would constitute a taking.

---

121 James v. Campbell, 104 U.S. 356, 357 (1882).

122 William Michael Treanor, *The Original Understanding of the Takings Clause and the Political Process*, 95 COLUM. L. REV. 782, 782 (1995) (citing Pennsylvania Coal v. Mahon, 260 U.S. 393, 415 (1922)).

123 Penn Cent. Transp. Co. v. New York City, 438 U.S. 104, 124 (1978).

124 Armstrong v. United States, 364 U.S. 40 (1959).

125 *Id.* at 48.

The Court's recent decision in *Knight v. Trump* fails to offer additional guidance but Justice Thomas's concurrence raises interesting questions regarding the legal status of platforms.[126] Despite granting a writ of certiorari, the Supreme Court declined to address the issue and instead remanded the case with directions to dismiss it as moot due to the change in administration.[127] In a concurring opinion, Justice Thomas acknowledges the difficulties with regulating social media platforms, specifically the question of whether they are common carriers and if the platforms themselves serve as public forums.[128] He presents two methods of regulating online platforms: the common carrier and public accommodations models.[129] The common carrier model states that because government offer common carriers "special privileges," they must "serve all comers."[130] The public accommodation model, citing the *Civil Rights Cases*, states that companies that hold themselves out to be open to the public may have their rights to exclude limited by the government.[131]

Moreover, other cases endorse the idea that the Takings Clause may apply to intangible property, such as data and algorithms. In *Ruckelshaus*, the Court held that intellectual property was property for the purpose of the Takings Clause.[132] The Court also noted that when dealing with "intangible" property, such as trade secrets "the extent of the property right therein is defined by the extent to which the owner of the secret protects his interest from disclosure to others."[133] The Court's decision in *Horne* also supported the idea that the Takings Clause provides equal protection to all types of private property, without any differentiation.[134]

---

126 In *Knight*, citizens sued Donald Trump, then President of the United States, alleging that blocking these users from interacting with his Twitter account violated the First Amendment because the Twitter comment threads under former-President Trump's tweets were a "public forum." Knight First Amend. Inst. at Columbia Univ. v. Trump, 928 F.3d 226, 226 (2019).

127 Biden v. Knight First Amend. Inst. at Columbia Univ., 141 S. Ct. 1220, 1220–21 (2021).

128 141 S. Ct. at 122–23.

129 *See id.* at 1222–24 ("In many ways, digital platforms that hold themselves out to the public resemble traditional common carriers. Though digital instead of physical, they are at bottom communications networks, and they 'carry' information from one user to another.").

130 *Id*. at 1222–23.

131 *Id*. at 1223.

132 Ruckelshaus v. Monsanto Co., 467 U.S. 986, 987 (1984).

133 467 U.S. at 1002.

134 Horne v Department of Agriculture, 135 S. Ct. 2419 (2015).

In summary, the Fifth Amendment's Takings Clause can pose a challenge for government regulation of technology companies, as significant limitations on the use of private property, such as those related to the regulation of platforms' use of automated systems, may be considered regulatory takings violations. This can make it difficult for governments to effectively regulate technology companies.

3. Perspectives from Legal Scholars: the Fifth Amendment and Regulating Automated Systems

According to legal experts, if government regulations significantly limit the use of private property, such as imposing restrictions on the use of automated systems, it may trigger the Fifth Amendment's Takings Clause, requiring the government to provide just compensation. This can create significant challenges for lawmakers and may make it impractical to pass legislation aimed at regulating online platforms' use of AI. This Section delves into the legal complexities that arise when regulating the use of automated systems by private companies and the potential for regulatory takings violations.

Nina I. Brown, an assistant professor at Syracuse University, and Jonathan Peters, an assistant professor at the University of Georgia Law School, argue that government regulations that dictate how platforms run trigger the Takings Clause because the regulations restrict the use of private property.[135] Platforms may argue that the legislation is fundamentally changing their property by preventing them from making content-related decisions that shape the platforms' communities.[136] If so, the amount of compensation would make it "practicably un-passable" for legislation to be passed to regulate social media platforms.[137]

For example, if Congress passed a law requiring platforms to host all users or to refrain from using recommendation algorithms, this would substantially change the operation and characteristics of the platforms. Platforms may then argue that the government's regulation materially interferes with their ability to use their property and decreases its economic value.[138] In the case

---

135 Nina I. Brown & Jonathan Peters, *Say This, Not That: Government Regulation and Control of Social Media*, 68 SYRACUSE L. REV. 521, 540–541 (2018).

136 Brown & Peters, *supra* note 135, at 542.

137 Brown & Peters, *supra* note 135, at 540–42.

138 Brown & Peters, *supra* note 135, at 542.

of recommendation algorithms, studies have shown their profitability and efficiency in managing platforms.[139] Additionally, the use of algorithms to monitor content reduces the need for human content moderators, thereby saving costs.[140] Consequently, regulation limiting their use may lead to the government having to pay the platforms the fair market value for the regulatory taking.

Other scholars agree that regulation of platforms violates the Fifth Amendment's Takings Clause.[141] lya Somin, a professor of law at George Mason University, finds that the Florida and Texas laws, [142] which attempted to constrain social media platforms' ability to remove content from their platforms, triggered the Takings Clause.[143]

Somin builds on Chief Justice Roberts reasoning in *Cedar Point* and distinguishes social media platforms from the shopping mall in *Pruneyard*.[144] In *Cedar Point*, the Court held that the California regulation, which allowed labor organizations to access an agricultural employer's property to solicit

---

139 *See* Aparna Das, Claire Mathieu & Daniel Ricketts *Maximizing Profit Using Recommender Systems*, WWW CONF. (2010) ("[[R]ecommendation systems] have been shown to help customers become aware of new products, increase sales and encourage customers to return to the business for future purchases.").

140 *See* Rem Darbinyan, Th*e Growing Role Of AI In Content Moderation*, FORBES (June 14, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/06/14/the-growing-role-of-ai-in-content-moderation/?sh=6c016e424a17 [https://perma.cc/AZ4D-E9AR] ("The ongoing increase in user-generated content makes it difficult for human moderators to deal with big volumes of information . . . Artificial intelligence (AI) can help optimize the content moderation process.").

141 *See* Ilya Somin, *Why the Florida and Texas Social Media Laws Violate the Takings Clause*, REASON (Sept. 17, 2022), https://reason.com/volokh/2022/09/17/why-the-florida-and-texas-social-media-laws-violate-the-takings-clause/ [https://perma.cc/26MR-HQKG] (arguing that social media laws in Florida and Texas mandate the occupation of private property without the owner's consent in violation of the Fifth Amendment).

142 *Id.*

143 *See id.*:

> The Florida and Texas social media laws are also blatant attacks on the right to exclude. No one doubts that the Twitter site and its various features are Twitter's private property. And the whole point of the Florida and Texas laws is to force Twitter and other social media firms to grant access to users and content the firms would prefer to exclude, particularly various right-wing users. Just as the plaintiffs in *Cedar Point* wanted to bar union organizers from their land, so Twitter wishes to bar some content it finds abhorrent (or that might offend or annoy other users).

144 Pruneyard Shopping Center v. Robins, 447 U.S. 74, 87–88 (1979):

> Most important, the shopping center by choice of its owner is not limited to the personal use of appellants. It is instead a business establishment that is open to the public to come and go as they please . . . We conclude that neither appellants' federally recognized property rights nor their First Amendment rights have been infringed by the California Supreme Court's decision . . .

support for unionization, was a per se physical taking.[145] In the opinion, Chief Justice Roberts drew a distinction between public and private and stated,

> The Board and the dissent argue that PruneYard shows that limited rights of access to private property should be evaluated as regulatory rather than per se takings. We disagree. Unlike the growers' properties, the PruneYard was open to the public, welcoming some 25,000 patrons a day. Limitations on how a business generally open to the public may treat individuals on the premises are readily distinguishable from regulations granting a right to invade property closed to the public.[146]

Thus, unlike the shopping malls in *Pruneyard*, social media platforms are not generally open to the public as they require profiles and thus are not required to host everyone's content. Twitter demonstrated this right in 2021 when it banned former President Donald Trump for violating its policies.[147]

Daniel A. Lyons, an assistant professor of law at Boston College Law School, argued that net neutrality violates the Takings Clause by effectively removing broadband providers' right to exclude others from their networks, which the Court's takings jurisprudence recognizes as one of the most important aspects of their property rights.[148] Lyons' argument was supported by a testimony at the Congressional Hearing before the Subcommittee on Communications and Technology of the Committee on Energy and Commerce ("Subcommittee").[149] The hearing concluded that the Federal Communications Commission's ("Commission") claim that the net neutrality network management rules do not pose any significant issues regarding the Fifth Amendment taking of a platform provider's property is erroneous.[150] This is because the net neutrality regulatory framework restricts the owner's ability to determine the most suitable way to manage traffic over its platform.[151] Similarly, regulation of automated systems that

---

145 Cedar Point Nursery v. Hassid, 141 S. Ct. 2063 (2021).

146 *Id.* at 2076–77.

147 X, *Permanent Suspension of @realDonaldTrump*, X BLOG (Jan. 8, 2021), https://blog.twitter.com/en_us/topics/company/2020/suspension [https://perma.cc/S9KB-ZY54].

148 Daniel A. Lyons, V*irtual Takings: The Coming Fifth Amendment Challenge to Net Neutrality Regulation*, 86 NOTRE DAME L. REV. 65, 68 (2011).

149 *Legislating to Safeguard the Free and Open Internet: Hearing before the Subcomm. on Commc'ns & Tech. of the Comm. on Energy and Com.*, 116th Cong., 155 n.111 (2020) [hereinafter Net Neutrality Hearing].

150 *Id.*

151 *Id.*

prevent an owner's ability to determine how to manage content on its platform may similarly trigger the Fifth Amendment.

In conclusion, regulating private companies' use of automated systems can result in regulatory takings violations, triggering the Fifth Amendment's Takings Clause and requiring costly compensation.

4. Fifth Amendment Considerations for the AI Bill of Rights

The Fifth Amendment's Takings Clause prohibits the government from passing regulations that substantially hinder one's property usage without just compensation. The AI Bill of Rights' Data Privacy and Human Alternatives principles could trigger the Takings Clause. The Data Privacy principle directs "[d]esigners, developers, and deployers" to allow individuals to decide how their data is collected, used, accessed, transferred, and deleted.[152] The Human Alternatives principle requires private parties using automated systems to allow users to opt out in favor of a human alternative.[153] While these principles aim to protect individual consumers, they may also substantially limit private parties' use of their intangible property.

a. Data Privacy Principle

Scholars have argued that data can be protected under the Takings Clause,[154] as it meets all the requirements of an asset under property laws.[155] Additionally, the AI Bill of Rights notes that there is an active market of data brokers, who buy and collected consumer data without consumers' permission or knowledge.[156] In the commentary section, the AI Bill of Rights

---

152 AI BILL OF RIGHTS, *supra* note 6, at 6.

153 AI BILL OF RIGHTS, *supra* note 6, at 7.

154 *See, e.g.*, Barbara J. Evans, *Much Ado About Data Ownership*, 25 HARV. J.L. & TECH. 69, 80 (2011) ("The public uses that can support a taking are quite broad and could include private, commercial research uses of data, if data were patient-owned."); *see also* Fred Cate & Robert E. Litan, *Constitutional Issues in Information Privacy* 7 (AEI-Brookings Joint Ctr. For Regul. Stud., Working Paper No. 01-11, 2001) ("Some commentators have suggested that the Supreme Court's recognition of these 'regulatory takings'—including takings of stored data—suggests that privacy regulations that substantially interfere with a private party's use of data that it has collected or processed, may require compensation under the Fifth Amendment.").

155 Paulius Jurcys, et al., *Ownership of User-Held Data: Why Property Law Is The Right Approach*, JOLT DIG. 1 (2021), https://jolt.law.harvard.edu/assets/digestImages/Paulius-Jurcys-Feb-19-article-PJ.pdf [https://perma.cc/2VU3-HC8P].

156 AI BILL OF RIGHTS, *supra* note 6, at 31.

correctly notes that legal limitations may prevent the deletion of data.[157] Thus, the requirement that those using automated systems delete all of the data or limit data usage may trigger the Takings Clause if it prevents the owner from extracting value from the digital property.

Consider TikTok to understand how legislation requiring compliance with the Data Privacy principle could impact owners of automated systems. TikTok's recommendation algorithm determines the videos presented to each user, and it collects various user metrics, such as uploaded images and videos, likes, comments, and passive behavior on the platform.[158] TikTok maintains that users own the rights to their intellectual property.[159] However, Takings Clause issues may arise if legislation is passed requiring TikTok to relinquish control of more systems related data (e.g., likes, scrolls, video interests, etc.).[160] The regulation may violate the Takings Clause as this data is necessary to ensure the effectiveness of the recommendation algorithm.

Additionally, data is rarely isolated. For example, if user A decides to delete their account, then user A's videos, likes, comments, and private information may easily be removed from the app. However, the application likely collected useful information relating to user A's habits on the application. The information may or may not be readily identifiable as user A. Still, the information is useful to the platforms' functionality, and

---

157 *See* AI BILL OF RIGHTS, *supra* note 6, at 33 ("Clear timelines for data retention should be established, with data deleted as soon as possible in accordance with legal or policy-based limitations.").

158 *See* Amarikwa, *supra* note 11, at 82 ("TikTok's recommendation algorithm also considers 'how many times [users] let a video loop, how quickly [users] scroll past certain content, and whether [users] are drawn to a particular category of effects and sounds.'"); *see also What is the 'For You' Feed?*, TIKTOK, https://www.tiktok.com/creators/creator-portal/en-us/how-tiktok-works/whats-the-for-you-page-and-how-do-i-get-there/ [https://perma.cc/E3AN-BS78] (last visited Apr. 2, 2023) ("The For You feed is all about you and making your TikTok experience personal. This stream of videos is curated to *your* specific interests, making it convenient to find videos and creators you love.").

159 *See Intellectual Property Policy*, TIKTOK (June 7, 2021), https://www.tiktok.com/legal/page/global/copyright-policy/en [https://perma.cc/NRH9-XDRG] ("TikTok respects the intellectual property rights of others . . . .").

160 Although this data may not include explicitly private information, such as name, social security number, etc., it is intimate. This information has allowed TikTok to identify people's sexual orientation without them disclosing such information. *See, e.g.*, Jess Joho, *Tiktok's Algorithms Knew I was Bi Before I Did. I'm Not the Only One*, MASHABLE (Sept. 18, 2022), https://mashable.com/article/bisexuality-queer-tiktok [https://perma.cc/A743-2WW5] (describing how TikTok's algorithms have perceived people's respective sexual orientations).

preventing a platform from maintaining this type of information, even when deidentified, may render the recommendation algorithm useless.

Several of the Data Privacy requirements appear in state privacy policies. For example, California's CCPA provides California residents with the right to access and portability[161] deletion,[162] correct inaccurate personal information,[163] information about collection and disclosure of personal information,[164] information about sales of personal information,[165] opt-out of sale of personal information,[166] and limit use and disclosure of sensitive personal information.[167] Although critics of the CCPA raised Takings Clause concerns, these concerns were never addressed in court.[168] This is likely because the CCPA's regulation does not interfere with the owner's reasonable investment-backed expectations. The CCPA only limits the use of sensitive personal information.[169] It is unclear if these rights would survive at the federal level.

Additionally, the CCPA's limitations on data sharing are not as far-reaching as those set out in the AI Bill of Rights' Data Privacy principle. While the CCPA permits individuals to request the deletion of their personal information, the provision only applies to personal information, and the CCPA's data restrictions do not impose significant regulatory action that would restrict or deprive the activity of its value, as is more likely to occur with the AI Bill of Rights.[170] This limited scope allows companies to continue utilizing other data they have collected.

---

161 CAL. CIV. CODE §1798.100 (West 2023).

162 CAL. CIV. CODE §1798.105 (West 2023).

163 CAL. CIV. CODE §1798.106 (West 2023).

164 CAL. CIV. CODE §1798.110 (West 2023).

165 CAL. CIV. CODE §1798.115 (West 2023).

166 CAL. CIV. CODE §1798.120 (West 2023).

167 CAL. CIV. CODE §1798.121 (West 2023).

168 *See* Joseph Jerome & Michelle De Mooy, *A New Day for Privacy Dawns in California*, CTR. FOR DEMOCRACY & TECH. (July 3, 2018), https://cdt.org/insights/a-new-day-for-privacy-dawns-in-california/ [https://perma.cc/E92G-FWJD] ("Critics of AB 375 have already raised the specter that the law's disclosure and deletion rights conflict with First Amendment and Takings Clause rights protected under the U.S. Constitution. The Takings Clause argument rests on the notion that regulations that substantially interfere with a business's use of data that it has collected or processed may require compensation under the Fifth Amendment.").

169 *Cf.* Penn Cent. Transp. Co. v. City of New York, 438 U.S. 104, 124 (1978) (mentioning factors considered in determining whether there is a Takings Clause violation).

170 CAL CIV. CODE § 1798.105 (West 2023).

Further issues arise when considering data sharing. The AI Bill of Rights indicates that "[e]ntities should receive consent before sharing data with other entities and should keep records of what data is shared and with whom."[171] Automated systems are developed using training data.[172] In some cases, the algorithm or automated system has been shown to reveal private information from the training data.[173] This issue raises questions of whether a law adopting the AI Bill of Right's Data Privacy principle will impose restrictions on the sale or licensing of automated systems. For example, if TikTok decided to license its recommendation algorithm, would the Data Privacy principle require TikTok to receive consent from all of its prior users who helped train or improve the algorithm's recommendations? The answer is unclear.[174]

The CCPA requires that when a user requests their data be deleted the company delete their personal information and also "notify any service providers or contractors to delete the consumer's personal information." [175] However, when licensing an automated system, the licensee may not modify the fundamental properties of the system but can instead adjust it to better fit their specific requirements.[176] Moreover, the FTC has recently used its powers to order algorithmic disgorgement or the deletion of an algorithm that was developed using improperly obtained data.[177] The FTC ordered Cambridge Analytica[178] to destroy its algorithm because it used consumer

171 AI BILL OF RIGHTS, *supra* note 6, at 35.

172 *See* Cass R. Sunstein, *The Use of Algorithms in Society*, REV. AUSTRIAN ECON. § 1 (2023) (raising the question of how much algorithms can be improved with additional data).

173 *See, e.g.,* Aneesh Tickoo, *How Safe Is the Data You1208 Use for Training Your Machine Learning Model?*, MARKTECHPOST (Apr. 28, 2022), https://www.marktechpost.com/2022/04/28/how-safe-is-the-data-you-use-for-training-your-machine-learning-model/ [https://perma.cc/PG9E-NT6E] ("A person given only the model's algorithm may reconstruct and deduce the sensitive information used to train the model in a variety of ways.").

174 *See* FED. TRADE COMM'N, CIVIL INVESTIGATIVE DEMAND ("CID") SCHEDULE 2 (FTC File No. 232-3044) (2023) (investigating data privacy issues associated with Large Language Models).

175 California Consumer Privacy Act of 2018, CAL. CIV. CODE. § 1798.105 (West 2023).

176 *See, e.g.*, *Transforming Work and Creativity with AI*, OPENAI, https://openai.com/product [https://perma.cc/94F6-VQQY] (last visited May 8, 2023) (offering ways for developers to adjust GPT-3 to fit their needs).

177 Joshua A. Goland, *Algorithmic Disgorgement: Destruction of Artificial Intelligence Models as the FTC's Newest Enforcement Tool for Bad Data*, 29 RICH. J.L. & TECH. 1, 2 (2023).

178 *See* McKenzie Funk, *Cambridge Analytica and the Secret Agenda of a Facebook Quiz*, N.Y. TIMES (Nov. 19, 2016), https://www.nytimes.com/2016/11/20/opinion/cambridge-analytica-facebook-quiz.html?searchResultPosition=6 [https://perma.cc/4QH5-REMZ] ("For several years, a data

data without getting the necessary notices and consents.[179] However, the FTC's authority is limited to unfair and deceptive practices.[180]

In summary, the AI Bill of Rights' Data Privacy principle does not necessarily impose an undue burden on those using or controlling automated systems. However, regulations that restrict data usage could still limit the ways in which platform owners can operate and diminish their economic interests, even if they do not amount to a full revocation of digital property rights. Therefore, while lawmakers have the authority to regulate data use, it is crucial that the scope and limits of data deletions are clearly defined to avoid ambiguity and potential conflicts with the Takings Clause.

b. Human Alternatives Principle

The Human Alternatives principle of the AI Bill of Rights may also violate the Takings Clause if adopted into law. The Human Alternatives principle directs private parties using automated systems to allow users to opt out of from automated systems in favor of a human.[181] The issue with the Human Alternatives principle is that it completely prevents private parties from using their automated systems in certain situations.

Determination of whether the regulation violated the Takings Clause would be a factual inquiry dependent on if the regulation substantially limited the private parties' ability to generate revenue. Given the principle recommends an opt-out option rather than an opt-in option,[182] a court will likely find that a Takings has not occurred unless the private party is able to show that regulation prevents them from generating a "reasonable return."[183]

---

firm eventually hired by the Trump campaign, Cambridge Analytica, has been using Facebook as a tool to build psychological profiles that represent some 230 million adult Americans.").

179 Cambridge Analytica, LLC, F.T.C. Docket No. 9383, 16 (Nov. 25, 2019).

180 Joshua A. Goland, *Algorithmic Disgorgement: Destruction of Artificial Intelligence Models as The FTC's Newest Enforcement Tool for Bad Data*, 29 RICH. J.L. & TECH. 1, 13 (2023).

181 AI BILL OF RIGHTS, *supra* note 6, at 7.

182 *See generally* Alan McQuinn, *The Economics of "Opt-Out" Versus "Opt-In" Privacy Rules*, INFO. TECH. & INNOVATION FOUND. (Oct. 6, 2017), https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules/ [https://perma.cc/N46U-3LD9] (discussing advantages of opt-out rules over opt-in ones).

183 *See* Penn Cent. Transp. Co. v. City of New York, 438 U.S. 104, 136 (1978) (relying on the petitioner's ability to generate a "reasonable return" in decision).

The application of the Takings Clause to deployers of automated systems is a complex and evolving area of law that poses challenges to regulators, platform owners, and users alike. The emerging use of AI and data-driven technologies has created new types of digital property that raise questions about the boundaries of the Takings Clause and the compensation owed for the taking of such assets.

The Data Privacy and Human Alternatives principles of the AI Bill of Rights may go too far and potentially trigger the Takings Clause. To avoid such fallacies, laws seeking to apply the Data Privacy principle should clearly delineate the type of data they seek to restrict and follow a CCPA model, which limits its scope to sensitive personal information. In the case of algorithms trained using personally sensitive information, deployers and developers should aim to get affirmative user consent prior to their use of the algorithm and where possible use anonymized or synthetic data[184] to train automated systems.

Additionally, laws requiring human alternatives face fewer issues than the Data Privacy principle laws as the algorithm may be used by a substantial amount of users. Still, to avoid issues, potential laws ought to be limited to opt-out options rather than an opt-out and human alternative. Human alternative options impose additional costs on the deployer of the automated systems that may result in the regulation preventing them from generating a reasonable return and thus violating the Takings Clause.

Therefore, while the Data Privacy and Human Alternative principles may be an ideal goal, the practicality of compensation makes the expansive versions of legislation highly impractical. Private parties may face significant obstacles in utilizing their intangible property when laws mandate data deletion, require human alternatives, or impose severe limitations on data usage.

CONCLUSION

This Comment highlights the growing concerns surrounding the use of AI and automated systems in decision making, especially by government agencies, and the potential implications of implementing the AI Bill of

184 *See* Melany Amarikwa, *Generative AI Will Not Solve Algorithmic Bias*, *in* A PROMETHEAN MOMENT: TOWARDS AN UNDERSTANDING OF GENERATIVE AI AND ITS IMPLICATIONS ON BIAS 8 (2023) (describing how Big Tech companies are turning to synthetic data to train their algorithms).

Rights. While the principles of the AI Bill of Rights represent a significant step towards ensuring the responsible development and deployment of AI in the US, there is a need to address potential constitutional issues that may arise from their implementation.

Specifically, this Comment highlights First and Fifth Amendment concerns and provides recommendations for lawmakers to mitigate these concerns. As AI continues to play an increasingly significant role in society, it is crucial that lawmakers strike a balance between protecting individual rights and promoting technological innovation.

The AI Bill of Rights is an important step toward guiding industries in the design, use, and deployment of automated systems in the US. However, it has faced criticism for its lack of enforcement measures and consideration for workers. Despite this, the AI Bill of Rights principles, like the FIPP, have the potential to influence future regulation.

The regulation of algorithmic speech is a notable concern that poses critical legal questions regarding the Compelled Speech Doctrine of the First Amendment. While some forms of algorithmic speech are generally considered to be constitutionally protected, regulating algorithmic speech based on the principles of the AI Bill of Rights may face challenges due to the Notice principle's requirements for documentation and explanations of outcomes.

Additionally, the regulation of automated systems usage raises legal questions regarding the Takings Clause of the Fifth Amendment. The adoption of the AI Bill of Rights' Data Privacy and Human Alternative principles into law may conflict with the Fifth Amendment's Takings Clause if it results in regulatory takings that substantially limit private parties' ability to use their intangible property.

In conclusion, the increasing use of automated systems in both public and private sectors necessitate the adoption of comprehensive guidelines in the US. While the AI Bill of Rights principles represent a crucial first step, further research and principles are needed to address the safety and equitable treatment of all Americans. As automated systems continues to evolve, it is crucial that lawmakers take active and proactive steps to develop regulations that balance innovation and the protection of individual rights.