Vanderbilt Journal of Entertainment & Technology Law

Volume 23 | Issue 1 Article 3

12-2020

Algorithmic Opacity, Private Accountability, and Corporate Social Disclosure in the Age of Artificial Intelligence

Sylvia Lu

Algorithmic Opacity, Private Accountability, and Corporate Social Disclosure in the Age of Artificial Intelligence

Sylvia Lu[*]

ABSTRACT

Today, firms develop machine-learning algorithms to control human decisions in nearly every industry, creating a structural tension between commercial opacity and democratic transparency. In many of their commercial applications, advanced algorithms are technically complicated and privately owned, which allows them to hide from legal regimes and prevents public scrutiny. However, they may demonstrate their negative effects—erosion of democratic norms, damages to financial gains, and extending harms to stakeholders—without warning. Nevertheless, because the inner workings and applications of algorithms are generally incomprehensible and protected as trade secrets, they can be completely shielded from public surveillance. One of the solutions to this conflict between algorithmic opacity and democratic transparency is an effective mechanism that requires firms to disclose information about their algorithms.

---

[*] J.S.D. (Doctor of Science of Law) Student, University of California, Berkeley, School of Law; Ph.D. Student, National Chengchi University. This Article was selected as the winning entry for the Berkeley Technology Law Journal 2020 Writing Competition Aldo J. Test Award. The author is tremendously grateful to Professor Sonia K. Katyal for her invaluable feedback during the development of this Article. Many special thanks, in alphabetical order, to Professors Kenneth A. Bamberger, Anupam Chander, Don Jeng, Ching-Fu Lin, Han-Wei Liu, Paul CB Liu, Laurent Mayali, Robert P. Merges, Paul M. Schwartz, Xiao-Fu Si, Huang-Chih Sung, Jane K. Winn, Se-Hwa Wu, Rosina Zapparoni, in addition to Dean Rowan, Lily D. Vo, and the staff of the *Vanderbilt Journal of Entertainment and Technology Law* for helpful comments and conversations at various stages in this project. Portions of this Article were presented at the BILETA 2020 Virtual Conference (Regulating Transitions in Technology and Law) in May 2020. The author wishes to thank the organizers and participants, in particular Professors Subhajit Basu, Marion Oswald, and Daithi Mac Sithigh, for this opportunity amid the COVID-19 Pandemic. The author welcomes feedback at swl@berkeley.edu. All errors remain my own.

This Article argues that the pressing problem of algorithmic opacity is due to the regulatory void of US disclosure regulations that fail to consider the informational needs of stakeholders in the age of artificial intelligence (AI). In a world of privately owned algorithms, advanced algorithms, as the primary source of decision-making power, have produced various perils for the public and firms themselves, particularly in the context of the capital market. While the current disclosure framework has not considered the informational needs associated with algorithmic opacity, this Article argues that algorithmic disclosure under securities law could be used to promote private accountability and further public interest in sustainability.

In this vein, through the lens of the US Securities and Exchange Commission (SEC) disclosure framework, this Article proposes a new disclosure framework for machine-learning-algorithm-based AI systems that considers the technical traits of advanced algorithms, potential dangers of AI systems, and regulatory governance systems in light of increasing AI incidents. Towards this goal, this Article considers numerous disclosure topics, analyzes key disclosure reports, and proposes new principles to help reduce algorithmic opacity, including stakeholder interests, sustainability considerations, comprehensible disclosure, and minimum necessary disclosure, ultimately striking a balance between democratic values in transparency and private interests in opacity. This Article concludes with a discussion of the impacts, limitations, and possibilities of using the new disclosure framework to promote private accountability and corporate social responsibility in the AI era.

TABLE OF CONTENTS

I. INTRODUCTION

The past decade has witnessed the private sector's dominance in developing algorithms.[1] Today, algorithms have flourished, presenting new business applications in nearly every industry.[2] From conventional commuting options to emergency medical treatments, algorithms have increasingly penetrated every corner of daily life, implying a foreseeable future in which they can influence every human decision.[3] Algorithms are becoming a primary source of decision-making power, but are often privately owned and inscrutable, which allows them to hide from legal regimes and prevents regulators from understanding and reviewing them. Thus, every service an algorithm performs—from data collection and training to business applications that have decision-making power over humans—may demonstrate a substantial degree of danger to the larger public.[4]

---

1. Since 2013, the number of AI start-ups and firms has strikingly increased, and investment in machine-learning systems tripled, leading to the growing influence of AI systems on high-tech industries. Xiaohong Quanieee & Jihong Sanderson, *Understanding the Artificial Intelligence Business Ecosystem*, 46(4) IEEE ENG'G MGMT. REV. 22, 22 (2018); Gil Press, *Top 10 Hot Artificial Intelligence (AI) Technologies*, FORBES (Jan. 23, 2017, 9:09 AM), https://www.forbes.com/sites/gilpress/2017/01/23/top-10-hot-artificial-intelligence-ai-technologies/#25b983f31928 [https://perma.cc/Z3HJ-UBPT] ("A Narrative Science survey found last year that 38% of enterprises are already using AI, growing to 62% by 2018. Forrester Research predicted a greater than 300% increase in investment in artificial intelligence in 2017 compared with 2016. IDC estimated that the AI market will grow from $8 billion in 2016 to more than $47 billion in 2020."); *see also* Dresner Advisory Services, 2019 DATA SCIENCE AND MACHINE LEARNING MARKET STUDY REPORT (2019), https://gumroad.com/l/dTfno [https://perma.cc/KC98-VMTP] ("[B]usiness units and IT departments are the likely centers of data science and machine learning oversight, with R&D ownership showing the fastest growth in 2019.").

2. AUTORITÉ DE LA CONCURRENCE & BUNDESKARTELLAMT, *Algorithms and Competition* 1, 1 (2019), https://www.autoritedelaconcurrence.fr/sites/default/files/algorithms-and-competition.pdf [https://perma.cc/FV7W-GG49] (recognizing big data and algorithms as the most important driving technological forces that revolutionize many sectors of the economy).

3. *See* Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 56 (2019) (noting that "algorithms determine the optimal way to produce and ship goods, the prices we pay for those goods, the money we can borrow, the people who teach our children, and the books and articles we read—reducing each activity to an actuarial risk or score."); Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson & Harlan Yu, *Accountable Algorithms*, 165 U. PA. L. REV. 633, 636 (2017); *see also* PETER STONE, RODNEY BROOKS, ERIK BRYNJOLFSSON, RYAN CALO, OREON ETZIONI, GREG HAGER, JULIA HIRSCHBERG, SHIVARAM KALYANAKRISHAN, ECE KAMAR, SARIT KRAUS, KEVIN LEYTON-BROWN, DAVID PARKES, WILLIAM PRESS, ANNALEE SAXENIAN, JULIA SHAH, MILIND TAMBE & ASTRO TELLER, ARTIFICIAL INTELLIGENCE AND LIFE IN 2030: ONE HUNDRED YEAR STUDY ON ARTIFICIAL INTELLIGENCE, REPORT OF THE 2015-2016 STUDY PANEL (2016).

4. Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183, 1186 (2019) ("[B]ecause their inner workings are often protected as trade secrets, they can remain entirely free from public scrutiny."); *see also* Jenna Burrell, *How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, 3 BIG DATA & SOC'Y 1

Employed in AI systems within a "black box," algorithms are accompanied by an opacity that has covertly led to problems affecting a wide range of stakeholders.[5] Since 2016, Facebook's AI-based services have been subject to ceaseless investigations, lawsuits, and class-action suits. Due to its operating results of advanced algorithms, Facebook has already been accused of data privacy violations,[6] fomenting division and inciting violence in Myanmar,[7] discrimination in Facebook's job-seeking service,[8] and breach of the Fair Housing Act.[9] On an individual level, many AI systems are prone to discriminate against minorities.[10] For instance, health care algorithms used to predict patient diseases discriminate against African Americans;[11] secret AI recruiting tools are biased against females;[12] and algorithms have been found to label homosexual and Jewish individuals negatively.[13] On a societal level,

(2016); Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085 (2018).

5. *See, e.g.*, FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 217–18 (2015); Anupam Chander, *The Racist Algorithm?*, 115 MICH. L. REV. 1023, 1029 (2017). For the purpose of this Article, stakeholders refer to those who play a key role in deciding the value of AI systems, including but not limited to investors, employees, algorithm developers, suppliers, and local communities.

6. Guy Rosen, *Security Update*, FACEBOOK NEWSROOM (Sept. 28, 2018, 9:41 AM), https://newsroom.fb.com/news/2018/09/security-update/ [https://perma.cc/632K-A7J8].

7. Alexandra Stevenson, *Facebook Admits It Was Used to Incite Violence in Myanmar*, N.Y. TIMES (Nov. 6, 2018), https://www.nytimes.com/2018/11/06/technology/myanmar-facebook.html [https://perma.cc/JB9J-EH5R].

8. Josh Eidelson, *Facebook Tools Are Used to Screen Out Older Job Seekers, Lawsuit Claims*, BLOOMBERG (May 29, 2018, 4:39 PM), https://www.bloomberg.com/news/articles/2018-05-29/facebook-tools-are-used-to-screen-out-older-job-seekers-lawsuit-claims [https://perma.cc/8MDZ-5928].

9. Terrence Dopp & Jesse Westbrook, *Facebook Violated Fair Housing Act with Ad Practice*, BLOOMBERG (Mar. 28, 2019, 7:13 PM), https://www.bloomberg.com/news/articles/2019-03-28/facebook-violated-fair-housing-act-with-ad-practice-hud-charges [https://perma.cc/TQU7-QYN9].

10. Katyal, *supra* note 3, at 69 ("Bad data, in other words, can perpetuate inequalities through machine learning, leading to a feedback loop that replicates existing forms of bias, potentially impacting minorities as a result.").

11. *Cf.* Monique Tello, *Racism and Discrimination in Health Care: Providers and Patients*, HARV. HEALTH BLOG, https://www.health.harvard.edu/blog/racism-discrimination-health-care-providers-patients-2017011611015 [https://perma.cc/9V5S-SYJC] (last updated July 9, 2020, 12:34 PM) (discussing the issue of health disparities resulting from racism and discrimination in the United States).

12. Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, REUTERS (Oct. 10, 2018, 6:04 PM), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showedbias-against-women-idUSKCN1MK08G [https://perma.cc/24JH-APAB].

13. Andrew Thompson, *Google's Sentiment Analyzer Thinks Being Gay Is Bad*, VICE (Oct. 25, 2017, 12:00 PM), https://www.vice.com/en_us/article/j5jmj8/google-artificial-intelligence-bias [https://perma.cc/JT4P-SY2U].

algorithms seem to absorb the biases, inequality, and even violence that ultimately plague society. This is particularly relevant in the COVID-19 Pandemic, where black patients and other minority individuals have been suffering and dying from COVID-19 at a disproportionate rate.[14] In all of these cases, algorithms that have the power to manipulate human decisions are shielded from public scrutiny due to the public's technical illiteracy and the trade secret protection algorithms receive. Despite a growing body of regulations in the United States, the law has failed to protect individual rights encroached upon by algorithms that are free from surveillance.[15] Within a decade, a growing number of AI-related incidents have emerged, demonstrating their erosion of democratic norms and harm to citizens, including discriminatory and unfair treatments with respect to individuals' employment, housing, and medical care.[16]

As consumers and citizens have struggled with incidents arising from opaque algorithms, corporate shareholders have also become victims of algorithmic opacity in business. While firms increasingly rely on algorithms as weapons to gain an advantage over competitors, the problem of algorithmic opacity has produced a number of deleterious outcomes for corporate shareholders and the capital market.[17] Without public scrutiny, algorithm-based services have led to a series of legal and managerial issues unanticipated by their corporate shareholders, particularly in the age of AI. For example, investors with significant stakes in AI businesses suffer from misuse of data and other AI-related misconduct that leads to enhanced remediation costs, reputation

14. *See, e.g.*, Eboni G. Price-Haywood, Jeffrey Burton, Daniel Fort & Leonardo Seoane, *Hospitalization and Mortality among Black Patients and White Patients with Covid-19*, 382 NEW ENG. J. MED. 2534 (2020), https://www.nejm.org/doi/10.1056/NEJMsa2011686?url_ver=Z39.88-2003&rfr_id=ori%3Arid%3Acrossref.org&rfr_dat=cr_pub++0pubmed [https://perma.cc/XG8E-G5TN].

15. Katyal, *supra* note 3, at 59 ("At the same time, the law can fail spectacularly to address this discrimination because of the rhetoric of objectivity and secrecy surrounding it."); *see* Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321, 1345 (1992).

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

17. Katia Porzecanski, *JPMorgan Commits Hedge Fund to AI in Technology Arms Race*, BLOOMBERG (July 2, 2019, 7:00 AM), https://www.bloomberg.com/news/articles/2019-07-02/jpmorgan-to-start-ai-hedge-fund-strategy-in-technology-arms-race [https://perma.cc/6WSC-992V] ("JPMorgan has spent billions in the technology arms race with rivals . . . deploying AI and machine-learning in investment banking and tapping industry experts to help shape strategy. . . . [O]ver the longer-term, [AI and machine-learning hedge funds have] outperformed other computer-driven funds.").

damage, and damage to their firms' long-term shareholder value.[18] In the previously mentioned case of Facebook, the Federal Trade Commission (FTC) imposed corporate governance reforms and fined Facebook a $5 billion penalty for violating the FTC's order by misrepresenting consumer privacy. This fine was the largest fine in the privacy sphere, representing 23 percent of Facebook's 2018 profit and was twenty times larger than the maximum General Data Protection Regulation (GDPR) fine.[19] Not only had Facebook's stock prices dropped to their lowest in nearly twenty-two months in November 2018,[20] but as of December 2018, Facebook was ranked the least trustworthy of the major high-tech firms.[21] Excluded from public oversight, algorithmic operations can also result in uncertain market conditions, immature business strategies, and changing regulatory environments, threatening the interests of corporate shareholders and adversely affecting consumers and the efficiency of the broader capital market.[22]

"Opacity culture" that dominates the development of new businesses is a major impediment to corporate accountability.[23] In the

---

18. *See* AUTORITÉ DE LA CONCURRENCE & BUNDESKARTELLAMT, *supra* note 2, at I (pointing out how advanced algorithms may have "detrimental effects on the competitive functioning of markets, especially by facilitating collusive practices.").

19. *See* Lesley Fair, *The FTC's $5 Billion Facebook Settlement: Record-Breaking and History Making*, FED. TRADE COMM'N BUS. BLOG (July 24, 2019, 8:52 AM), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history [https://perma.cc/R8SM-L3NB]; Aarti Shahani & Avie Schneider, *FTC to Hold Facebook CEO Mark Zuckerberg Liable for Any Future Privacy Violations*, NPR (July 24, 2019, 12:16 PM), https://www.npr.org/2019/07/24/741282397/facebook-to-pay-5-billion-to-settle-ftc-privacy-case [https://perma.cc/DUD8-V836]; *What if My Company/Organisation Fails to Comply with Data Protection Rules?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-company-organisation-fails-comply-data-protection-rules_en [https://perma.cc/RLQ7-Q6XJ] (last visited Sept. 15, 2020). Some of the FTC Commissioners even considered this fine as insufficient to deter Facebook from future violations, as Facebook may have earned billions of dollars due to violations of the FTC order. *See* Dissenting Statement of Commissioner Rohit Chopra at 15–16, *In re* Facebook, Inc. (2019), No. 182-3109, 2019 WL 3451729 (F.T.C.) (2019); Dissenting Statement of Commissioner Rebecca Kelly Slaughter at 2, *In re* Facebook, Inc., No. 182-3109, 2019 WL 3451729 (F.T.C.) (2019).

20. Salvador Rodriguez, *Here Are the Scandals and Other Incidents that Have Sent Facebook's Share Price Tanking in 2018*, CNBC (Nov. 20, 2018, 10:22 PM), https://www.cnbc.com/2018/11/20/facebooks-scandals-in-2018-effect-on-stock.html [https://perma.cc/63CX-64PM].

21. Sarah Feldman, *Facebook Loses the Public's Trust*, STATISTA (Dec. 14, 2018), https://www.statista.com/chart/16431/tech-company-trust/ [https://perma.cc/KJN3-PALV].

22. *See generally* Saqib Aziz & Michael Dowling, *Machine Learning and AI for Risk Management*, *in* DISRUPTING FINANCE 33 (Theo Lynn et al. eds, 2019) (exploring how machine learning and AI solutions are transforming risk management in the private sector).

23. *See* Merritt B. Fox, *Required Disclosure and Corporate Governance*, 62 L. & CONTEMP. PROBS. 113, 116 (1999); Elliot J. Weiss, *Disclosure and Corporate Accountability*, 34 BUS. LAW. 575, 576–77 (1979) ("Disclosure . . . is the oil that lubricates the machinery of the governance

field of corporate governance, scholars, regulators, and stakeholders have long viewed disclosure regulations as an effective mechanism to ensure corporate accountability.[24] In the United States, disclosure regulations are the responsibility of multiple government agencies, including the Securities and Exchange Commission (SEC).[25] As a lead agency protecting the capital market and investor interests, the SEC emphasizes transparency as a responsibility of every market participant and cooperates with government agencies, market participants, and investors to monitor opacity threats.[26] Although the SEC has established disclosure requirements for public firms, the current disclosure framework does not consider the informational needs associated with algorithmic opacity.

Because the emerging risks caused by algorithms are so revolutionary, potentially catastrophic, and messier than before, this Article argues that firms should adequately disclose the operating results of their algorithms not only concerning the interests of their investors but also those of other stakeholders in AI systems.[27] Similar to climate change concerns that justify SEC sustainability disclosures, algorithms with considerable social risks should also legitimize disclosure as a requisite for firms that develop advanced algorithms.[28] Riskier than cyberattacks that legitimize the SEC cybersecurity

---

system."); *Sustainable Investment Joins the Mainstream*, ECONOMIST (Nov. 25, 2017), https://www.economist.com/finance-and-economics/2017/11/25/sustainable-investment-joins-the-mainstream [https://perma.cc/8FP2-E4F7].

24. Fox, *supra* note 23, at 116; Weiss, *supra* note 23, at 577; *Sustainable Investment Joins the Mainstream*, *supra* note 23.

25. *See* Troy A. Paredes, *Blinded by the Light: Information Overload and Its Consequences for Securities Regulation*, 81 WASH. U. L.Q. 417, 427 (2003).

26. *See Structured Disclosure at the SEC: History and Rulemaking*, U.S. SEC. EXCH. COMM'N, https://www.sec.gov/page/osdhistoryandrulemaking [https://perma.cc/KMG4-HJHD]. (last updated May 21, 2020). For an analysis of the SEC's performance on enforcing securities law, see Stavros Gadinis, *The SEC and the Financial Industry: Evidence from Enforcement Against Broker-Dealers*, 67 BUS. LAW. 679 (2012).

27. Stakeholders call for "an assessment of how AI systems can be made transparent, predictable and verifiable so as to effectively prevent distortion, discrimination, manipulation and other forms of improper use." AUTORITÉ DE LA CONCURRENCE & BUNDESKARTELLAMT, *supra* note 2, at 77; *see also* VERBRAUCHERZENTRALE BUNDERSVERBAND, *Algorithmic Decision Making for the Benefit of Consumers*, 1, 3–4, https://www.vzbv.de/sites/default/files/downloads/2019/07/19/19-06-25_vzbv_positions_adm_control_summary_en.pdf [https://perma.cc/DC44-NDUP] (last visited Nov. 10, 2019).

28. *See* Commission Guidance Regarding Disclosure Related to Climate Change, Exchange Act Release No. 34-61469, 75 Fed. Reg. 6290 (Feb. 8, 2010) (codified at 17 C.F.R. §§ 211, 231, 241) [hereinafter SEC Guidance on Climate Change Disclosure].

disclosure,[29] advanced algorithms are unprecedentedly causing danger to every corner of daily life,[30] and thus desperately necessitate algorithmic disclosure in the current landscape of corporate disclosure.[31]

To fill this regulatory void, this Article explores how a disclosure framework in securities laws could be used to encourage algorithmic accountability and transparency in the age of AI. As the current disclosure framework has failed to consider the information needs associated with algorithmic opacity, this Article argues that algorithmic disclosure in the context of corporate governance could further corporate shareholder and public interest in sustainability.[32] By proposing a new algorithmic disclosure framework integrated with mandatory and recommended disclosure requirements that take account of commercial, technical, and social considerations in accountability, this Article hopes to better align capital markets with algorithmic accountability and sustainability.

After a brief introduction to AI in Part II, this Article discusses how algorithms are applied in privately owned AI systems by looking at three critical industries: financial services, medical services, and transportation services. Part III turns to the issues of technical and legal algorithmic opacity, examines how democratic norms, such as privacy, equality, and safety, have been traded for algorithmic opacity, and discusses how the existing law responds to dangers derived from algorithm-based services in each context. Turning toward the disclosure framework in the context of SEC securities laws, Part IV investigates how current practices apply to AI systems. Since the current disclosure framework fails to consider the informational needs of stakeholders in AI systems, this Article proposes a new disclosure framework for advanced-algorithm-based AI systems that takes into account commercial, technical, and social considerations to meet the needs of stakeholders in the digital age. Part VI concludes with a brief discussion

---

29. *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Exchange Act Release No. 34-82746, 83 Fed. Reg. 8166 (Feb. 26, 2018) (codified at 17 C.F.R. §§ 229, 249) [hereinafter SEC Statement and Guidance on Cybersecurity Disclosures].

30. *See* Hin-Yan Liu, *The Power Structure of Artificial Intelligence*, 10 L. INNOVATION & TECH. 197, 205 (2018).

31. THE IEEE GLOBAL INITIATIVE ON ETHICS OF AUTONOMOUS AND INTELLIGENT SYSTEMS, ETHICALLY ALIGNED DESIGN: A VISION FOR PRIORITIZING HUMAN WELL-BEING WITH AUTONOMOUS AND INTELLIGENT SYSTEMS 7, 159 (2017).

32. Corporate sustainability refers to a business enterprise's creation of long-term value both for its economic profits as well as the benefits of stakeholders affected by its commercial practices or policies. For an in-depth discussion of different definitions of corporate sustainability, see Marcel van Marrewijk, *Concepts and Definitions of CSR and Corporate Sustainability*, 44(2) J. BUS. ETHICS 95 (2002).

of the impacts, limitations, and possibilities of using the algorithmic disclosure framework to regulate algorithmic opacity toward accountability and sustainability in the AI era.

II. ARTIFICIAL INTELLIGENCE AND ALGORITHMS

To solve the problems of algorithmic opacity, it is necessary to understand AI and algorithms. AI refers to a form of intelligent computing that employs algorithms to maximize its chance of solving problems or achieving goals.[33] Based on computational intelligence, algorithms can undertake intellectual activities, such as perception, inference, reasoning, learning, and adapting.[34] AI systems are a class of algorithms that reflect varying degrees of human-like consciousness, autonomy, and intelligence. On a continuum between tool-like and human-like systems, the least advanced AI systems depend on preprogrammed rules to evaluate options or make decisions.[35] In contrast, more advanced AI systems utilize a class of machine-learning algorithms.[36] Unlike rule-based AI systems, machine-learning-based AI systems rely on the algorithm's dynamic ability to learn from data, identify patterns, make inferences, and reach solutions without explicit instructions or human intervention.[37] A subset of machine-learning algorithms is "deep learning," which employs artificial neural networks that imitate human neural networks.[38] Deep-learning algorithms can

33. *See* Future of Artificial Intelligence Act of 2017, H.R. 4625, 115th Cong. § 3(a) (2017).

34. *See* TOSHINORI MUNAKATA, FUNDAMENTALS OF THE NEW ARTIFICIAL INTELLIGENCE 1 (2008) (explaining the competencies of AI that include inference, reasoning, perception, learning, control, prediction, classification, and optimization).

35. A traditional algorithm depends on rules defined by human experts and "takes some input and some logic in the form of code and drums up the output." Richa Bhatia, *How Does Machine Learning Differ from Traditional Algorithms*, ANALYTICS INDIA MAG. (Oct. 9, 2018), https://analyticsindiamag.com/how-do-machine-learning-algorithms-differ-from-traditional-algorithms/ [https://perma.cc/FA6A-44CW].

36. Dresner Advisory Services, *supra* note 1 ("advanced initiatives related to data science and machine learning, such as data mining, advanced algorithms, and predictive analytics"); *see* Louis Columbus, *State of AI and Machine Learning in 2019*, FORBES (Sept. 8, 2019, 2:38 PM), https://www.forbes.com/sites/louiscolumbus/2019/09/08/state-of-ai-and-machine-learning-in-2019/#78edaf6e1a8d [https://perma.cc/3BSL-5UUV].

37. For an introduction to recent advances in machine-learning algorithms, see Andreas Holzinger, Markus Plass, Michael Kickmeier-Rust, Katharina Holzinger, Gloria Cerasela Crişan, Camelia-M. Pintea & Vasile Palade, *Interactive Machine Learning: Experimental Evidence for the Human in the Algorithmic Loop*, 49(7) APPLIED INTELLIGENCE 2401 (2019).

38. For recent breakthroughs in deep learning techniques, see Yann LeCun, Yoshua Bengio & Geoffrey Hinton, *Deep Learning*, 521 NATURE 436 (2015); Bernard Widrow & Michael A. Lehr, *30 Years of Adaptive Neural Networks: Perceptron, Madaline, and Backpropagation*, 78 PROCS. IEEE 1415 (1990).

process data through multiple layers to identify patterns and extract concepts.[39]

The advancement of data storage, process, and analysis technologies is the engine of powerful algorithms, which rely heavily on raw data to provide solutions.[40] For example, machine-learning algorithms—the subset of algorithms extensively used by the private sector—need sufficient data to reach solutions.[41] In a business context, AI systems in particular require massive amounts of data to understand customer needs and requirements. Facebook, Google, and Amazon use significant amounts of raw data to continually refine their products and services, which in turn attracts more users and yields even more data.[42]

Additionally, technology that helps effectively acquire and process data also plays a crucial role in the success of powerful AI systems. For instance, Internet of Things (IoT) devices, such as smartphones, allow millions of human speech samples to be recorded and processed by AI hardware.[43] Combined with algorithms encompassing machine-learning techniques, IoT systems continually evolve and improve their effectiveness.[44] In addition, computing power technologies, such as expert systems and machine learning, allow AI systems to address a vast number of problems with superior capability.[45] The integration of cloud computing also facilitates the storing of data and provides a platform to create and test AI systems.[46] With progressive algorithmic improvement and copious amounts of data used to extract meaning, the power of AI systems continues to rise significantly.

---

39. LeCun et al., *supra* note 38, at 436 ("Deep learning allows computational models that are composed of multiple processing layers to learn representations of data with multiple levels of abstraction.").

40. Manheim & Kaplan, *supra* note 16, at 121–22.

41. *See* Michael Chui, Nicolaus Henke & Mehdi Miremadi, *Most of AI's Business Uses Will Be in Two Area*s, HARV. BUS. REV. (July 20, 2018), https://hbr.org/2018/07/most-of-ais-business-uses-will-be-in-two-areas [https://perma.cc/ZHG5-9B6R].

42. Gil Press, *How Apple, Amazon, Facebook, Google and Microsoft Made 2018 the Year that IT Mattered A Lot*, FORBES (Dec. 30, 2018, 9:45 AM), https://www.forbes.com/sites/gilpress/2018/12/30/how-apple-amazon-facebook-google-and-microsoft-made-2018-the-year-that-it-mattered-a-lot/#6d68e9761cee [https://perma.cc/KG8R-GXPC].

43. Quanieee & Sanderson, *supra* note 1, at 22–23.

44. *See id.*

45. *See id.* at 23.

46. *See generally* Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623, 1626–34 (discussing the use of the cloud). For an introduction to the technological distinctions among different models of cloud computing, see Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1690, 1694–95 (2018).

A. Algorithms and AI Systems in the Private Sector

Over time, the business applications of AI systems have tremendously increased. Currently, the use of AI systems has almost become every technology firm's focus of development, quickly transforming commercial services and products.[47] In commercial practices, algorithms are being integrated into products and services that exhibit varying degrees of automated functions.[48] AI technology has penetrated a number of industries, including transportation, telecommunications, financial services, medical services, retail, and real estate, among others.[49] With human-like reasoning and inference abilities, AI systems perform tasks and provide solutions for firms to build products, services, or business models in various industrial sectors.[50] With machine-learning algorithms, some AI systems can continually improve at a speed unmatched by human beings.[51] Firms are also utilizing AI systems as a tool to better understand customer complaints and needs.[52] Currently, algorithm-based commercial functions play a key role in financial services, transportation, and medical services.

1. Financial Services

In financial services, algorithms are transforming retail investments and credit. As an example, robot advisory services, like Betterment, provide an online financial advisor that offers clients financial management suggestions and optimal investment strategies.[53] Robot advisory services are based on algorithms that collect and parse client information regarding clients' past performance and risk preferences.[54] Such business applications of AI systems have

---

47. Bernard Marr, *Why Every Company Needs an Artificial Intelligence (AI) Strategy for 2019*, FORBES (Mar. 21, 2019, 1:23 AM), https://www.forbes.com/sites/bernard-marr/2019/03/21/why-every-company-needs-an-artificial-intelligence-ai-strategy-for-2019/#6ef657a368ea [https://perma.cc/6URB-MF6J].

48. *Id.*

49. STONE ET AL., *supra* note 3, at 4.

50. *Id.*

51. *See, e.g.*, Chris Baraniuk, *The Cyborg Chess Players that Can't Be Beaten*, BBC FUTURE (Dec. 4, 2015), https://www.bbc.com/future/article/20151201-the-cyborg-chess-players-that-cant-be-beaten [https://perma.cc/HVH5-7DMP] (discussing how the computing power of AI is succeeding against chess grandmasters).

52. Quanieee & Sanderson, *supra* note 1, at 23.

53. *Choosing a Robo-Advisor: Investing Made Personal*, BETTERMENT, https://www.better-ment.com/category/robo-advisor/ [https://perma.cc/747S-74NQ] (last visited Sept. 12, 2020).

54. *See* Tom Baker & Benedict Dellaert, *Regulating Robo Advice Across the Financial Services Industry*, 103 IOWA L. REV. 713, 718, 726 (2018).

disrupted traditional advising practices by offering personalized digital investment advice to clients at a low cost.[55]

Similarly, AI systems coupled with machine-learning algorithms are showing a remarkable ability to capture, process, and utilize data factored into credit calculations. Several digital lenders have made predictions of borrowers' creditworthiness based on machine-learning algorithms.[56] At the request of digital lenders, borrowers install applications to their digital devices, allowing algorithms to track and obtain comprehensive data on their mobile devices.[57] In this way, digital lenders can access borrowers' social media profiles, the types of computers they use, their shopping preferences, and the places they have visited, which allow algorithms to underwrite consumer credit risk.[58]

2. Transportation Services

Algorithms have revolutionized the transportation industry with the creation of Global Positioning System (GPS) technology and driverless cars. The integration of massive amounts of data, real-time sensing, and connectivity technology has led to the success of GPS systems and driverless cars by improving traffic and route predictions.[59] With GPS technology, drivers are guided by stored map information that can choose an optimal route based on the shortest path algorithm.[60] At the same time, the GPS navigation system collects information about transportation patterns and provides the collected data to firms.[61]

Currently, vehicles have a variety of capabilities that integrate real-time sensing and decision-making functions, such as airbag control systems that protect driver safety by using algorithms that can detect

---

55. *See Overview of Betterment's Pricing*, BETTERMENT (Sept. 1, 2018), https://www.betterment.com/resources/pricing-overview/ [https://perma.cc/349L-NQ97] (last visited Sept. 12, 2020).

56. Shlomit Yanisky-Ravid & Sean K. Hallisey, *"Equality and Privacy by Design": A New Model of Artificial Intelligence Data Transparency Via Auditing, Certification, and Safe Harbor Regimes*, 46 FORDHAM URB. L.J. 428, 466–67; *see* William Magnuson, *Financial Regulation in the Bitcoin Era*, 23 STAN. J.L. BUS. & FIN. 159, 183–84 (2018).

57. Matt Hamblen, *Lenders May Eye Smartphone Use Before Giving You a Loan*, COMPUT. WORLD (Dec. 4, 2015, 11:01 AM), https://www.computerworld.com/article/3012140/lenders-may-eye-smartphone-use-when-deciding-on-loans.html [https://perma.cc/226L-7B7K].

58. *See id.*

59. *See* Jeffrey L. Duffany, *Artificial Intelligence in GPS Navigation Systems*, *in* 1 2010 2ND INTERNATIONAL CONFERENCE ON SOFTWARE TECHNOLOGY AND ENGINEERING V1-382 (Houssain Kettani & Yang Li eds., 2010).

60. *See id.* at V1-386.

61. *See* Joe Grengs, Xiaoguang Wang & Lidia Kostyniuk, *Using GPS Data to Understand Driving Behavior*, 15 J. URBAN TECH. 32, 32, 34 (2008).

crashes to trigger airbags.[62] Driven by advances in machine-learning algorithms' ability to perceive their surroundings, tech giants, such as Waymo, Nvidia, Tesla, and Uber, have created autonomous cars.[63] As of July 2019, Waymo's autonomous cars logged more than ten billion miles.[64] Additionally, Tesla's autopilot can drive autonomously, while requiring drivers to monitor the car and take control on short notice.[65] In the near future, advances in algorithms' sensing and reasoning abilities will be followed by improvements in machine-learning driving-assist algorithms.[66] When coupled with advanced algorithms, the self-driving car can reduce drivers' navigating chores, traffic congestion, and accidents caused by human error.[67] In the future, algorithms employed by autonomous vehicles may eventually be applied to other types of transportation like remote-controlled trucks or flying cars.[68]

3. Medical Services

AI systems in medical services are concerned with employing algorithms to emulate human perception in processing health data without direct human intervention. Today, algorithms have been applied to a wide range of medical services, including diagnosis processes, treatment decision support, patient monitoring, surgery assistance, new drug development, personalized medicine and care, and management of health care systems.[69] Recently, successful AI health care has been closely associated with the use of data and machine-learning algorithms. For example, data has been collected

62. William J. Fleming, *New Automotive Sensors: A Review*, 8(11) IEEE SENSORS J. 1900, 1909 (2008).

63. *See* Andrea Miller, *Some of the Companies That Are Working on Driverless Car Technology*, ABC NEWS (Mar. 21, 2018, 2:03 PM), https://abcnews.go.com/US/companies-working-driverless-car-technology/story?id=53872985 [https://perma.cc/6UBS-SL4R].

64. Darrell Etherington, *Waymo Has Now Driven 10 Billion Autonomous Miles in Simulation*, TECH CRUNCH (July 10, 2019, 4:17 PM), https://techcrunch.com/2019/07/10/waymo-has-now-driven-10-billion-autonomous-miles-in-simulation/ [https://perma.cc/KT35-YWCB].

65. *Autopilot and Full Self-Driving Capability*, TESLA, https://www.tesla.com/support/autopilot (last visited Oct. 4, 2019).

66. STONE ET AL., *supra* note 3, at 20.

67. *Id.* at 20–21.

68. Antony Riley, *The Algorithm at the Heart of Autonomous Truck Safety*, MEDIUM (Jan. 27, 2018), https://medium.com/@antonyriley/the-algorithm-at-the-heart-of-autonomous-truck-safety-5be09203e5dc [https://perma.cc/VKN6-MJKH]; Jack Stewart, *Airbus Uses Lasers to Teach Its Flying Car to Land*, WIRED (Aug. 23, 2017, 9:00 AM), https://www.wired.com/story/airbus-vahana-flying-car-landings/ [https://perma.cc/K6LX-KX9P].

69. *The AI Industry Series: Top Healthcare AI Trends to Watch*, CB INSIGHTS, https://www.cbinsights.com/research/report/ai-trends-healthcare/ [https://perma.cc/S8AU-N6Q5] (last visited Nov. 10, 2019); *see* Quanieee & Sanderson, *supra* note 1, at 23.

from social media profiles to predict users' health risks through machine-learning algorithms, and robots are being used in surgical procedures.[70] With algorithms, millions of patient medical records can be mined to produce more accurate diagnoses and effective treatments.[71] Data from wearable devices can also be a valuable source for creating personalized medical diagnoses.[72] For example, Enlitic, a machine-learning company, builds deep-learning algorithms to develop medical services that streamline radiology diagnoses.[73] The firm uses a deep-learning platform to analyze medical data, including but not limited to patient medical records, radiology images, blood tests, and genomics to generate diagnoses that consider patients' personal situations.[74] The AI firm PathAI also uses machine-learning algorithms to help pathologists produce more precise cancer diagnoses for patients.[75] The firm uses algorithms to analyze high volumes of patients with greater accuracy in diagnoses and developing methods for individualized medical treatments.[76]

From the financial industry to the health care industry, algorithms are gaining importance in the private sector, quickly reshaping commercial services and human lives. Collectively, these developments suggest a near future in which algorithms affect every action or decision made by humans. Despite their growing influence, the inner workings of algorithms are often unavailable for public investigation, operated by firms in opacity.[77] The opacity of algorithms is derived from algorithms' inherent complexity as well as a legal

---

70. Sam Daley, *32 Examples of AI in Healthcare that Will Make You Feel Better About the Future*, BUILT IN, https://builtin.com/artificial-intelligence/artificial-intelligence-healthcare [https://perma.cc/F8QL-SU5Z] (last updated July 29, 2020); Arunima Roy, Katerina Nikolitch, Rachel McGinn, Safiya Jinah, William Klement & Zachary A. Kaminsky, *A Machine Learning Approach Predicts Future Risk to Suicidal Ideation From Social Media Data*, NPJ DIGIT. MED., May 26, 2020, at 1.

71. Krista Conger, *Computers Trounce Pathologists in Predicting Lung Cancer Type, Severity*, STAN. MED. NEWS CTR. (Aug. 16, 2016), https://med.stanford.edu/news/all-news/2016/08/computers-trounce-pathologists-in-predicting-lung-cancer-severity.html [https://perma.cc/G85N-VDFZ].

72. STONE ET AL., *supra* note 3, at 27.

73. *See Enlitic Brings Deep Learning Diagnostic Solutions to the Radiological Society of North America*, ENLITIC (Nov. 14, 2016), https://www.enlitic.com/enlitic-brings-deep-learning-diagno [https://perma.cc/7C2S-LRUB].

74. *Id.*

75. Emily Inverso, *Medicine Gets Digital: How Data Is Pushing Healthcare Forward*, FORBES (Oct. 2, 2017, 11:43 AM), https://www.forbes.com/sites/emilyinverso/2017/10/02/medicine-gets-digital-how-data-is-pushing-forward-healthcare/#18b7b29a13f7 [https://perma.cc/M5CC-FT42].

76. PATHAI, https://www.pathai.com/ (last visited Sept. 14, 2020).

77. Michael Luca, Jon Kleinberg & Sendhil Mullainathan, *Algorithms Need Managers, Too*, HARV. BUS. REV., Jan.–Feb. 2016, at 98.

system that allows algorithms to operate in secrecy.[78] Without public surveillance, algorithmic opacity has led to a number of issues that negatively affect consumers, investors, other individual stakeholders, and society as a whole.

III. THE PERILS OF ALGORITHMIC OPACITY

Advancements of algorithms have manifested the hazards of AI systems throughout the private sector. As AI systems use algorithms to perceive the world, the opacity problems with algorithms are quietly expanding in the business world with the support of machine-learning algorithms.[79] The following Section discusses the nature of algorithmic opacity, looks into the perils of algorithmic opacity that involve social, economic, and technical concerns, and explains why such dangers require information disclosure for public oversight.[80]

A. Algorithmic Opacity

Algorithmic opacity is defined as the lack of visible processes to scrutinize the inner workings and resulting applications of algorithms.[81] Algorithmic opacity can take the form of technical opacity or legal opacity. Technical opacity typically occurs in advanced machine-learning algorithms, whereas legal opacity is pervasive regardless of the type of algorithm.[82] Both types of opacity can prevent stakeholders and government agencies from understanding and monitoring the design and application of algorithms that involve a number of ethical, legal, and managerial issues. The issue of algorithmic opacity, broadly termed as a "black box" by Professor Frank Pasquale, refers to the invisibility and complexity of advanced algorithms that hinder effective investigation of AI systems.[83]

---

78. *See* Burrell, *supra* note 4, at 3–5; *see also* Han-Wei Liu, Ching-Fu Lin & Yu-Jie-Chen, *Beyond* State v. Loomis*: Artificial Intelligence, Government Algorithmization and Accountability*, 27 INT'L J.L. & INFO. TECH. 122 (2019) (discussing the unsolved challenges of legal black box as well as technical black box associated with the rise of data analytics and algorithms).

79. Burrell, *supra* note 78, at 1–12; Liu et. al., *supra* note 78.

80. Burrell, *supra* note 78, at 1–12; Liu et. al., *supra* note 78.

81. *See* Pragya Paudyal & B.L. William Wong, *Algorithmic Opacity: Making Algorithmic Processes Transparent Through Abstraction Hierarchy*, 62 PROC. HUM. FACTORS & ERGONOMICS SOC'Y ANN. MEETING 192, 193 (2018).

82. For instance, during its learning process, a neural network doesn't "break down handwritten digit recognition into subtasks that are readily intelligible to humans." Burrell, *supra* note 4, at 6.

83. *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015).

1. Technical Opacity

Technical opacity occurs in machine-learning algorithms in which evolving computational processes are too complicated for humans to understand.[84] Because the data structure of machine-learning algorithms continually evolves, the inner workings of algorithms are difficult to analyze, particularly in terms of how results are reached.[85] For example, in a deep-learning algorithm, the neuron network is composed of layers of neurons working in a loose manner to reach a decision.[86] Here, the algorithm's structure can be incomprehensible to human cognition. At the same time, the neural network learns from experience, making its decision-making process even more intuitive, complex, and thus unpredictable.[87] The technical opacity inherent in machine-learning algorithms thus allows algorithms to learn and adapt without human understanding or control.[88] Accordingly, as "the Godfather of Deep Learning" Geoffrey Hinton observes, "[a] deep-learning system doesn't have any explanatory power . . . the more powerful the deep-learning system becomes, the more opaque it can become."[89]

2. Legal Opacity

Unlike technical opacity in machine-learning algorithms, legal opacity occurs across a wider range of algorithms, regardless of the subset of algorithms involved. The origin of legal algorithmic opacity is the result of legal structures that provide overlapping intellectual

---

84. *See* IAN GOODFELLOW, YOSHUA BENGIO & AARON COURVILLE, DEEP LEARNING 1–4 (2016) (explaining how the tasks undertaken by AI projects, such as image recognition, data pattern identification, or language processing, may be easy for humans to perform, but hard to describe); *see also* Davide Castelvecchi, *Can We Open the Black Box of AI?*, NATURE (Oct. 5, 2016), https://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731 [https://perma.cc/K42N-YBM8].

85. *See* GOODFELLOW ET AL., *supra* note 84, at 1–2; *see also* Castelvecchi, *supra* note 84.

86. *See* GOODFELLOW ET AL., *supra* note 84, at 13–16. Currently, a neuron network may, at the high end, consist of hundreds of thousands of interconnected artificial neurons working to reach a decision. *See id*. at 21–22.

87. Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 HARV. J.L. & TECH. 889, 897 (2018) (noting that advanced machining-learning algorithms are capable of learning from data and experiences that produce unforeseeable decision-making process and results).

88. *See* Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513, 532, 539 (2015) (discussing the unpredictable behaviors of robots that "can lead to solutions no human would have come to on her own").

89. Siddhartha Mukherjee, *A.I. Versus M.D.*, NEW YORKER (Apr. 3, 2017).

property protection in algorithms.[90] Currently, the inner workings and applications of algorithms are generally protected by firms as trade secrets, and thus hidden from public scrutiny.[91] As Professor Sonia Katyal recently observed, this current state is the result of a drawback of intellectual property law that incentivizes trade secrecy of algorithms.[92]

For decades, algorithms were independently protected by three intellectual property regimes—copyright law, patent law, and trade secret law.[93] At different periods, each regime has dominated the protection in algorithms, but the law of trade secrecy has most consistently reigned. Firms have relied on trade secret law since the early years of software development, as it provided necessary protection against misappropriation.[94] Later, despite the subsequent rises and falls of both copyrightability and patentability for algorithms,[95] courts became reluctant to provide patent protection for algorithms.[96] While the copyright regime tends to protect the secrecy of source code, courts have limited copyrightability in algorithms due to their functionality;[97] trade secret law thus continues to dominate the landscape of algorithms protection.[98]

---

90. Katyal, *supra* note 4, at 1190 ("[S]oftware garnered a unique position within the law: it remains one of the few spheres to enjoy concurrent protections from trade secrecy, copyright law, and patent law.").

91. *Id.* at 1236. ("As a result of these shortcomings of intellectual property protection to incentivize disclosure and access, source code remains entirely secluded from outside view, maximizing the developer's control, irrespective of whether the goals of third party access lie in innovation, competition, or investigation.").

92. *Id.* at 1227, 1236.

93. *Id.* at 1190.

94. *Id.* at 1190, 1227; *see also* Richard Raysman, *Protection of Proprietary Software in the Computer Industry: Trade Secrets as an Effective Method*, 18 JURIMETRICS J. 335, 344 (1978).

95. *See* Pamela Samuelson, *Staking the Boundaries of Software Copyrights in the Shadow of Patents*, 71 FLA. L. REV. 243 (2019).

96. Even though there has been a rise of open-source movement, trade secrets remain developers' primary avenue for software protection. In the 1980s, courts in the United States began to admit copyrightability of algorithms and attempted to broaden the scope of copyright protection, but at the same time struggled to limit copyrightability in algorithms due to their functionality. Katyal, *supra* note 4, at 1203–07, 1216–25; *see also* Philip J. Weiser, *Law and Information Platforms*, 1 J. ON TELECOMMS. & HIGH TECH. L. 1, 6–16, 22–31 (2002) (discussing the open-source movement).

97. During the 1960s, the United States Patent Office refused patents for algorithms. It was not until the 1981 case of *Diamond Diehr* that courts decided to acknowledge software patentability. Since then, the courts further extended the boundary of software patentability in several cases, such as *Alappat*, *State Street*, and *AT&T*. In response to the overbroad boundaries of software protection, the courts and Congress began to narrow software patentability in cases including *In re Bilski* and *Alice*. After *Alice*, courts tended to oppose granting patents for software, which were often characterized as abstract ideas. Katyal, *supra* note 4, at 1216–25.

98. *Id.* at 1225.

There are several reasons for the domination of trade secret protection of algorithms over patent and copyright law. First, compared to the changing and uncertain boundaries of patent and copyright, trade secret law provides more stable protection for developers to secure their legal rights and averts risks of losing protection.[99] Second, while both patent and copyright law encourage a certain extent of information disclosure, trade secret law promotes opacity that is more aligned with firms' strategic and marketing needs.[100] Third, an algorithm is a form of specialized information that can be naturally free from public interpretation and difficult to reverse engineer,[101] which allows firms to maintain their secrecy at a lower cost.[102] Fourth, copyright and patent regimes are less beneficial to algorithms, as copyright law does not provide an exclusive right prohibiting others from independently creating similar algorithms, and patent law fails to protect algorithms once the functional architecture of an algorithm is modified and falls outside the original claims of the patent.[103] For these reasons, trade secret law has become the most favorable avenue for firms to protect algorithms, and even those derived from the public domain have been claimed as trade secrets.

Furthermore, algorithms can maintain core secrecy at all times, even if they only fall under the protection of patent or copyright law.[104] As Professor Katyal observes, although copyright and patent law encourage dissemination of information, neither require "disclosure of much of the source code."[105] Accordingly, under the protection of intellectual property law, firms are incentivized to keep the process and business applications of algorithms secret, raising a number of concerns for larger stakeholders in the context of business applications.

B. The Values Compromised by Algorithmic Opacity: Privacy, Equality, and Safety

Algorithmic opacity has led to a number of harmful outcomes to society that threaten democratic norms and stakeholder interests.

---

99. *Id.* at 1216.

100. James Gibson, *Once and Future Copyright*, 81 NOTRE DAME L. REV. 167, 177–78 (2005).

101. *See* Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrecy as IP Rights*, 61 STAN. L. REV. 311, 338–41 (2008).

102. Katyal, *supra* note 4, at 1214; Lemley, *supra* note 101, at 333–34.

103. INT'L TECH. L. ASS'N, RESPONSIBLE AI: A GLOBAL POLICY FRAMEWORK 263 (2019), https://www.itechlaw.org/sites/default/files/Responsible_AI.pdf [https://perma.cc/A8TS-SB4P].

104. Katyal, *supra* note 4, at 1226 ("[S]ource code remains secret at all times, irrespective of whatever regime it falls under.").

105. *Id.* at 1188.

There are three concrete, fundamental rights of citizens endangered by algorithmic opacity: privacy, equality, and safety. Based on the increasing pervasiveness of machine-learning-based business applications in financial services, transportation services, and medical services, the following Sections use these services as representative examples to discuss how existing laws and regulations respond to the emerging problems posed by algorithmic opacity.

1. Trading Privacy for Opacity

In AI firms, algorithms crafted to further consumer interests can simultaneously sacrifice consumer privacy if they operate without adequate oversight. The foundation of powerful algorithms is access to data. The more relevant information there is in an accessible data set, the more capable algorithms are of performing a task or making an effective decision.[106] However, incentivized by current legal structures, firms often collect and use consumer data without supervision when building AI systems. For example, IoT technologies allow firms to obtain large quantities of data in numerous databases and are often used to facilitate the collection and analysis of consumer data.[107] Once a massive amount of consumer data has been collected, algorithms can use that data to influence or control consumers in AI systems.[108] Despite the IoT providing virtually every movement of consumers to firms, the collection and use of consumer data remains opaque.[109] This opacity leads to significant information asymmetry with consumer privacy as the unknowing victim.

Similarly, in the case of financial services, consumers unknowingly trade their private information for AI services. Digital lenders often require borrowers to install cell phone applications that constantly track and collect data in users' digital devices, including information concerning social media profiles, website visit history, and shopping preferences, among others.[110] Landlords and retailers use

106. *See Artificial Intelligence: What It Is and Why It Matters*, SAS INST., https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html [https://perma.cc/8KWK-HJ3H] (last visited Oct. 3, 2020).

107. Manheim & Kaplan, *supra* note 16, at 123 (discussing how IoT is being utilized in the private sector and how the application of IoT produces information asymmetry).

108. Dirk Helbing, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael Hagner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zicari & Adrej Zwitter, *Will Democracy Survive Big Data and Artificial Intelligence?*, SCI. AM. (Feb. 25, 2017), https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/ [https://perma.cc/PZL6-ABBQ].

109. Manheim & Kaplan, *supra* note 16, at 123.

110. *See also* Jennifer Valentino-Devries, Natasha Singer, Michael H. Keller & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES

data collected from mobile phones to pinpoint their target customers.[111] Moreover, Amazon sells facial-scan technology that analyzes customers' faces to detect their reactions to and interests in displays and products.[112] US shopping centers have started to adopt technology that collects information on consumers' behavior patterns, facial features, and lengths of stay.[113]

The large-scale collection and use of data can erode information privacy and even manipulate decisional privacy—the autonomy to make decisions about private actions without intrusion or intervention.[114] Firms collect consumer data to examine the behavior patterns of consumers, feed their algorithms, and use them to tailor products, services, and advertisements that target consumers' income levels for private benefit.[115] Retailers use algorithms to track consumers' moves and reactions in shopping malls to improve product displays and marketing.[116] Firms increasingly use consumers' private information for their commercial profits, often secretly.[117] The way firms use algorithms to target consumers according to their income levels, desires, and needs constitutes a subtle form of manipulation known as "behavioral marketing."[118] Behavioral marketing covertly surrenders informational privacy; such manipulation may gradually erode individuals' free will to make decisions.[119]

(Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/F58L-AD93].

111. James Green, *3 Ways Customer Data Allows for Pinpoint Marketing*, ENTREPRENEUR (July 24, 2015), https://www.entrepreneur.com/article/247372 [https://perma.cc/7NAN-2ARZ].

112. Kate Fazzini, *Amazon's Facial Recognition Service Is Being Used to Scan Mugshots, but It's Also Used to Track Innocuous Things Like Soccer Balls*, CNBC (Dec. 6, 2018, 11:13 PM), https://www.cnbc.com/2018/12/06/how-amazon-rekognition-works-and-what-its-used-for.html [https://perma.cc/KE4V-ZASN].

113. Esther Fung, *Shopping Centers Exploring Facial Recognition in Brave New World of Retail*, WALL ST. J. (July 2, 2019, 8:00 AM), https://www.wsj.com/articles/shopping-centers-exploring-facial-recognition-in-brave-new-world-of-retail-11562068802 [https://perma.cc/K4C3-EMSY].

114. *See* ROGER J.R. LEVESQUE, *Decisional Privacy*, *in* ADOLESCENCE, PRIVACY, AND THE LAW: A DEVELOPMENTAL SCIENCE PERSPECTIVE 16 (2016).

115. *See* Eden Gillespie, *Are You Being Scanned? How Facial Recognition Technology Follows You, Even as You Shop*, GUARDIAN (Feb. 23, 2019, 9:11 PM), https://www.theguardian.com/technology/2019/feb/24/are-you-being-scanned-how-facial-recognition-technology-follows-you-even-as-you-shop [https://perma.cc/U7WR-25NH]; DANIEL J. SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW 803–04 (6th ed. 2018).

116. Fung, *supra* note 113.

117. *See* Gillespie, *supra* note 115.

118. For a discussion of legal issues surrounding online behavioral advertising, see Steven C. Bennett, *Regulating Online Behavioral Advertising*, 44 J. MARSHALL L. REV. 899 (2011).

119. Manheim & Kaplan, *supra* note 16, at 130 (arguing that online behavioral advertising subverts consumers' free will and erodes consumers' autonomy to make decisions).

In the United States, the government has not enacted federal legislation that regulates how much firms should disclose concerning their usage of algorithms and how to obtain consent in terms of individual data collection.[120] At the federal level, although numerous statutes provide privacy protection, different statutes regulate different industries, forming a complex regulatory landscape.[121] For instance, the Health Insurance Portability and Accountability Act (HIPAA) is the primary act that requires protection of patient privacy, which limits the types of medical records that can be utilized in algorithms to some extent.[122] However, as Professors Daniel Solove and Paul Schwartz describe, there is no federal statute directly regulating personal information collected by most businesses.[123] Currently, the FTC is the primary agency regulating privacy in the United States, with the power to prohibit "unfair or deceptive acts or practices in or affecting commerce."[124] Although the FTC has issued a set of principles on the use of online behavioral marketing,[125] without binding regulations in place, only firms conducting unfair or deceptive business practices can be investigated.[126] This is inadequate because such a regulatory sanction does not apply to firms' large-scale collection and use of data that may ultimately surrender consumers' information privacy or decisional privacy. While Congress has held hearings on the subject, no bills have been passed to fill the void.[127]

On the other hand, some states have stricter privacy statutes than federal laws,[128] such as California, which passed the strongest privacy protections in the United States so far.[129] Recently,

120. For the US system of consumer data privacy regulation, see SOLOVE & SCHWARTZ, *supra* note 115, at 786–90.

121. *Id.* at 786.

122. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 262(a), 110 Stat. 1936 (codified in scattered sections of 26, 29, and 42 U.S.C.).

123. SOLOVE & SCHWARTZ, *supra* note 115, at 786–87.

124. Federal Trade Commission Act, Pub. L. No. 93-637, sec. 201(a), § 5(a), 88 Stat. 2193, 2193 (1914) (codified as amended at 15 U.S.C. § 45(a)). For a further discussion of the FTC's approach to policing the marketplace, see Paul M. Schwartz, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 147–50 (2017).

125. *See* FED. TRADE COMM'N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 46–47 (2016), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400 behavadreport.pdf [https://perma.cc/TKP2-K56W].

126. *See* Federal Trade Commission Act, *supra* note 124.

127. Manheim & Kaplan, *supra* note 16, at 131.

128. SOLOVE & SCHWARTZ, *supra* note 115, at 789.

129. Passed in 2018, the California Consumer Privacy Act provides consumer protection for residents of California, regardless of where the data is processed. *See* CAL. CIV. CODE § 1798.140(c) (2018).

Washington, Texas, and Illinois passed bills to protect privacy with respect to biometric information, followed by others considering measures that would protect faces and other physical attributes.[130] Although some states have attempted to regulate firms' controversial business practices, few laws and regulators are given power to regulate borderless digital practices that may erode privacy norms.[131] Accordingly, AI firms are only self-regulated, which means in some contexts few or no sanctions combat the increasing privacy invasions arising from opaque commercial applications.[132]

2. Trading Equality for Opacity

The health care industry has been one of the industries that has witnessed the growing number of AI business applications and their extending harms to equality produced by algorithmic opacity.[133] From predicting who will be diagnosed with cancer to deciding who will receive medical treatment, algorithms are increasingly making decisions that humans would have made.[134] However, since the ways in which the health care industry collects and uses data are kept from public oversight, algorithms have been found to replicate systemic discrimination present in the data and perpetuate disparities.[135]

Algorithm-based health care systems can replicate bias in a number of ways. Risk-prediction algorithms built on patient health records can reproduce discrimination already deeply rooted in society. Machine-learning algorithms may underrepresent or overrepresent patient cohorts, creating discriminatory AI systems and inferior treatment of minorities. Racial discrimination has been replicated by algorithms in the health care industry, affecting access to medical treatment for millions of Americans.[136] Recently, a study published in

---

130. Molly K. McGinlyey & Kenn Brotman, *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States*, NAT'L L. REV. (Mar. 25, 2019), https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states [https://perma.cc/5DJB-KGWL].

131. *See* Manheim & Kaplan, *supra* note 16, at 161.

132. SOLOVE & SCHWARTZ, *supra* note 115, at 787.

133. *See* Daley, *supra* note 70.

134. Yanisky-Ravid & Hallisey, *supra* note 56, at 431–32 (illustrating "[m]any decisions previously determined by humans are now made by autonomous AI systems").

135. *See* Ziad Obermeyer, Brian Powers, Christine Vogeli & Sendhil Mullainathan, *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 (6464) SCIENCE 447, 447 (2019); Irene Dankwa-Mullan, *Examining Health Disparities in Precision Medicine*, IBM (Oct. 14, 2019), https://www.ibm.com/blogs/watson-health/examining-health-disparities-in-precision-medicine/ [https://perma.cc/KQ82-KNR3].

136. Kara Manke, *Widely Used Health Care Prediction Algorithm Biased Against Black People*, BERKELEY NEWS (Oct. 24, 2019), https://news.berkeley.edu/2019/10/24/widely-used-health-

Science found that the Impact Pro program—an AI system developed by a health care firm—prioritizes white patients over black patients by giving black patients unreasonably low risk scores despite their poorer health conditions.[137] This study showed that bias in algorithms has affected over half of the black patients who should have access to high-risk health care management programs and that these algorithms have been found to discriminate against at least a hundred million US citizens in their health care decisions.[138] In another example, a study on hypertrophic cardiomyopathy revealed that genetic misdiagnoses can cause health disparities.[139] In research on a cardiac disease commonly caused by gene mutations, Black Americans were more frequently misclassified as pathogenic, although they received positive reports for the genetic variants.[140] During the COVID-19 Pandemic, structural racism replicated by advanced algorithms also contributed to unequal treatment in the health care industry and consequently increased the risks COVID-19 poses for people of color.[141] As the Black Lives Matter movement brings the issue of biases to the forefront, more and more research indicates that black people are more likely to suffer serious illness and death from COVID-19 than white people, in part due to their limited access to medical treatment.[142] In all these cases, because firms develop their AI systems in a black box, the hidden bias embedded in firm-owned algorithms has been difficult to detect and eliminate. As a result of these discriminatory AI health care services operating in opacity, minorities end up receiving inferior health care

---

care-prediction-algorithm-biased-against-black-people/?fbclid=IwAR21ND23XtA6GZXKLBe15SajborPwJaGi2gksEek7o5Ju1Kea9JM1lf3IiE [https://perma.cc/DUN6-AZMR].

137. *See* Obermeyer et al., *supra* note 135.

138. *Id.* at 447–49.

139. Arjun K. Manrai, Birgit H. Funke, Heidi L. Rehm, Morten S. Olesen, Bradley A. Maron, Peter Szolovitz, David M. Margulies, Joseph Loscalzo & Isaac S. Kohane, *Genetic Misdiagnoses and the Potential for Health Disparities*, 375 NEW ENG. J. MED. 655, 656 (2016).

140. *Id.*

141. *US: Covid-19 Disparities Reflect Structural Racism, Abuses: Human Rights Watch Testimony to US House of Representatives Ways and Means Committee*, HUM. RIGHTS WATCH (June 10, 2020), https://www.hrw.org/news/2020/06/10/us-covid-19-disparities-reflect-structural-racism-abuses [https://perma.cc/5NAJ-FSDG].

142. Kristen MJ Azar, Zijun Shen, Robert J. Romanelli, Stephen H. Lockhart, Kelly Smits, Sarah Robinson, Stephanie Brown & Alice R. Pressman, *Disparities in Outcomes Among COVID-19 Patients in a Large Health Care System in California*, 39 HEALTH AFFS. 1253 (2020); Roni Caryn Rabin, *Black Coronavirus Patients Land in Hospitals More Often, Study Finds*, N.Y. TIMES (May 23, 2020), https://www.nytimes.com/2020/05/23/health/coronavirus-black-patients.html [https://perma.cc/8Q2V-C5UK]; Sherita Hill Golden, *Coronavirus in African Americans and Other People of Color*, JOHNS HOPKINS MED., https://www.hopkinsmedicine.org/health/conditions-and-diseases/coronavirus/covid19-racial-disparities [https://perma.cc/SCR3-XHQ8].

treatment and become sicker due to inequalities reproduced by algorithms.

Even in the health care industry, the US government has adopted a conservative approach to regulating inequality. To date, there are few nondiscrimination rules applying to the development of machine-learning algorithms and the use of AI systems.[143] The Genetic Information Nondiscrimination Act (GINA) prohibits insurance firms from using genetic information to deny employment.[144] However, regulations designed for AI medical services that require continual review are lacking.[145] Currently, the Food and Drug Administration (FDA) has been hesitant to approve innovative health care AI systems because of the underlying safety risks and unknown cost-benefit trade-offs of AI systems.[146]

Even in such a strict regulatory environment, algorithmic opacity derived from algorithm-based medical services brings consistent dangers of inequality, which are difficult to investigate and are not necessarily illegal.[147] As Optum, an AI health care company, has admitted, algorithms empowered to make medical decisions for humans should be continually reviewed, refined, and provided with socioeconomic information.[148] Yet without binding legislation and regulations, industry standards that prioritize profit over the public

---

143. For the paucity of the principle of nondiscrimination that applies to algorithms, see Katyal, *supra* note 3, at 100–03.

144. *See* Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (codified in scattered sections of 29 and 42 U.S.C.).

145. *See* AI NOW INST., AI NOW REPORT 2018, at 23–24, 30–32.

146. *See* Charles Aunger, *Should the FDA Regulate AI?*, FORBES (Aug. 14, 2019, 9:45 AM), https://www.forbes.com/sites/forbestechcouncil/2019/08/14/should-the-fda-regulate-al/#3088165c39a0 [https://perma.cc/PSM5-MZKQ] ("In 2014, the FDA approved AI-based algorithms for medical use, and in 2018, it issued its first approval of an AI system for diagnosis without human clinical input."); *see also* Conor Hale, *FDA Delivers Regulatory Guidance on AI Software and Clinical Decision-Making Aids*, FIERCEBIOTECH (Sept. 26, 2019), https://www.fiercebiotech.com/medtech/fda-delivers-regulatory-guidance-ai-software-and-clinical-decisionmaking-aids [https://perma.cc/SBW4-D4KN] ("[T]he FDA said it plans to focus oversight on higher-risk software functions, including those used in serious or critical situations—as well as machine learning-based algorithms, where the program's logic and inputs may not be fully explained to the user.").

147. Katyal, *supra* note 3, at 97.

148. Carolyn Y. Johnson, *Racial Bias in a Medical Algorithm Favors White Patients over Sicker Black Patients*, WASH. POST (Oct. 24, 2019, 1:00 PM), https://www.washingtonpost.com/health/2019/10/24/racial-bias-medical-algorithm-favors-white-patients-over-sicker-black-patients/ [https://perma.cc/V44Q-L893] ("'Predictive algorithms that power these tools should be continually reviewed and refined, and supplemented by information such as socio-economic data, to help clinicians make the best-informed care decisions for each patient,' Optum spokesman Tyler Mason said.").

good are unlikely to change.[149] Accordingly, algorithms can reproduce and deepen inequities in health care or other industries as long as they are owned by firms and are proprietary in nature, making it difficult for stakeholders and governments to monitor them.[150]

3. Trading Safety for Opacity

Algorithms develop rapidly to serve humans. However, without adequate surveillance, their misbehaviors or malfunctions may cause injury or death, either because hurting humans can achieve their set goal, or they are simply miscalculated.[151]

Concerns about safety can be traced to the invisible use of data, the unknown programming of algorithms, and the unforeseeable and uncontrolled features of some machine-learning algorithms. As stated above, the workings of algorithms depend heavily on the input of data.[152] When the input of data is ambiguous, biased, or falsified, output becomes erroneous and unreliable.[153] If the veracity and neutrality of data go unverified, algorithms can amplify wrong information when utilized in a business context, similar to the discrimination problem seen in algorithm-based medical services.[154]

When the algorithms of an AI system are deficient, risks will inevitably arise, as AI systems are only as good as the quality of their algorithms.[155] In a business context, algorithms may struggle when reacting to scenarios unanticipated by their programming or when the data input is insufficient for them to reach effective solutions. In the case of robot advisory services, if market environments are uncertain, algorithms may risk offering suboptimal or harmful operating results.

---

149. *Id.*

150. Katyal, *supra* note 3, at 59 (discussing how inequalities replicate existing bias through machine learning and adversely impact minorities).

151. *See, e.g.*, Faiz Siddiqui, *Tesla Floats Fully Self-Driving Cars as Soon as This Year. Many Are Worried About What That Will Unleash*, WASH. POST (July 17, 2019, 9:16 PM), https://www.washingtonpost.com/technology/2019/07/17/tesla-floats-fully-self-driving-cars-soon-this-year-many-are-worried-about-what-that-will-unleash/ [https://perma.cc/97PA-74RT].

152. *See, e.g.*, Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 680, 688 (2016).

153. *Id.*

154. Kroll et al., *supra* note 3, at 680 ("These decision rules are machine-made and follow mathematically from input data, but the lessons they embody may be biased or unfair nevertheless.").

155. Willem Sundblad, *Data Is the Foundation for Artificial Intelligence and Machine Learning*, FORBES (Oct. 18, 2018, 10:30 AM), https://www.forbes.com/sites/willemsundbladeurope/2018/10/18/data-is-the-foundation-for-artificial-intelligence-and-machine-learning/#65bca29451b4 [https://perma.cc/X8BG-FN2F] ("Any application of AI and ML will only be as good as the quality of data collected.").

Accordingly, such algorithms may increase risks rather than further consumer interests and business efficiency.

Furthermore, machine-learning algorithms are designed with features that implicate their unpredictability and the inability to control them because their solutions are based on subsequent experiences and not limited by preset rules.[156] Even if the programming of algorithms is clear and understandable, the interplay between massive data and that programming creates complexity beyond human comprehension.[157] Additionally, because the decision logic of machine-learning systems changes according to their post-design experiences, even the human that develops the algorithms can neither control nor predict their actions.[158] In this context, control is difficult to maintain, as machine-learning algorithms adapt and learn based on their subsequent experiences.[159]

Given the invisible operation of data and algorithms that hinders the surveillance of AI systems, a number of safety concerns have been identified in the private sector. As exemplified by autonomous vehicle incidents, algorithms have caused several serious injuries. In the driverless car industry, algorithms performing decision-making tasks are privately designed and tested on humans, often with little public surveillance.[160] In 2018, Uber confirmed that a woman was killed by one of its self-driving cars, which failed to "see" her when navigating the Phoenix suburbs.[161] Tesla's autonomous vehicle killed a driver in an accident caused by its autopilot

156. *See* Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategie*s, 29 HARV. J.L. & TECH. 353, 365 (2016); Burrell, *supra* note 4, at 5.

157. Anjanette H. Raymond, Emma Arrington Stone Young & Scott J. Shackelford, *Building a Better HAL 9000: Algorithms, the Market, and the Need to Prevent the Engraining of Bias*, 15 NW. J. TECH. & INTELL. PROP. 215, 220–21 (2018) ("Machine learning, by contrast, is used to analyze patterns and then apply results to decision making and actions. All computing processes, from mining to learning, in some sense rely on algorithms, but their scope, complexity, and conceptual accessibility varies widely.").

158. Scherer, *supra* note 156, at 365–66.

159. *See id.* at 366.

160. Faiz Siddiqui, *Silicon Valley Pioneered Self-Driving Cars. But Some of Its Tech-Savvy Residents Don't Want Them Tested in Their Neighborhoods*, WASH. POST (Oct. 3, 2019, 10:16 AM), https://www.washingtonpost.com/technology/2019/10/03/silicon-valley-pioneered-self-driving-cars-some-its-tech-savvy-residents-dont-want-them-tested-their-neighborhoods/ [https://perma.cc/MCL8-E5XG] ("California has awarded permits to 63 different companies to test self-driving vehicles on state roads, according to state figures from Aug. 9.").

161. Sam Levin & Julia Carrie Wong, *Self-Driving Uber Kills Arizona Woman in First Fatal Crash Involving Pedestrian*, GUARDIAN (Mar. 19, 2018, 6:48 PM), https://www.theguardian.com/technology/2018/mar/19/uber-self-driving-car-kills-woman-arizona-tempe [https://perma.cc/ZH2D-XEQQ].

technology.[162] Neither firm substantially suffered from these incidents. In the Uber incident, although Uber had disabled the car's automatic-brake systems, the assisting driver was found liable for the incident.[163]

In spite of these fatal incidents, few federal laws have been enacted to monitor the development of these algorithms.[164] Recently, Waymo, a self-driving car company, launched new plans for an "early rider program," which invites volunteer residents to be driverless car test subjects.[165] The National Transportation Safety Board (NTSB) is the lead US governmental agency responsible for the investigation of civil transportation accidents, but it has no legal authority to require firms to implement its recommendations.[166] Some scholars suggest that self-driving cars should be regulated under the existing legal system, where car incidents occur without the engagement of machine-learning algorithms. Alternatively, some argue that legal doctrines and liability rules should treat humans and AI systems differently.[167] Currently, self-driving car accidents have not been classified into a specific

---

162. Sean O'Kane, *Tesla Hit with Another Lawsuit over a Fatal Autopilot Crash*, VERGE (Aug. 1, 2019, 5:59 PM), https://www.theverge.com/2019/8/1/20750715/tesla-autopilot-crash-law-suit-wrongful-death [https://perma.cc/QP7C-S6WC] ("Tesla is being sued by the family of a 50-year-old man who died in a crash while using the company's Autopilot advanced driver assistance system. . . . Banner is the fourth known person to die while using Autopilot, and his family is the second to sue Tesla over a fatal crash involving the technology. . . . The similarities [of Tesla's fatal Autopilot crashes] suggest that Tesla didn't address this issue with Autopilot's ability to recognize a crossing tractor-trailer, regardless of the potential fault of the driver.").

163. David Shepardson, *Update 3-NTSB Cites Uber, Distracted Backup Driver in Fatal Self-Driving Crash*, YAHOO! FIN. (Nov. 19, 2019), https://finance.yahoo.com/news/1-u-safety-board-chair-192153357.html [https://perma.cc/W8HW-U5QE].

164. AI NOW INSTIT., *supra* note 145, at 23.

165. Ellice Perez, *Getting Ready for More Early Riders in Phoenix*, WAYMO (Aug. 21, 2018), https://blog.waymo.com/2019/08/getting-ready-for-more-early-riders-in.html [https://perma.cc/95L6-YVWV].

166. *See Safety Recommendations*, NAT'L TRANSP. SAFETY BD., https://www.ntsb.gov/safety/safety-recs/_layouts/ntsb.recsearch/RecTabs.aspx [https://perma.cc/FT57-B8ZR] ("Safety recommendations are issued by the NTSB following the investigation of transportation accidents and the completion of safety studies. Recommendations usually address a specific issue uncovered during an investigation or study and specify how to correct the situation.").

167. For further discussions, see Edmond Awad, Sohan Dsouza, Richard Kim, Jonathan Schulz, Joseph Henrich, Azim Shariff, Jean-François Bonnefon & Iyad Rahwan, *The Moral Machine Experiment*, 563 NATURE 59 (2018); Jason Millar, *Ethics Settings for Autonomous Vehicles*, *in* ROBOT ETHICS 2.0: FROM AUTONOMOUS CARS TO ARTIFICIAL INTELLIGENCE 20 (Patrick Lin et al. eds., 2017); Jeffrey Gurney, *Imputing Driverhood: Applying a Reasonable Driver Standard to Accidents Caused by Autonomous Vehicles*, *in* ROBOT ETHICS 2.0: FROM AUTONOMOUS CARS TO ARTIFICIAL INTELLIGENCE 51 (Patrick Lin et al. eds., 2017); Bryan Casey, *Amoral Machines, or: How Roboticists Can Learn to Stop Worrying and Love the Law*, 111 NW. U. L. REV. 231 (2017); Andrea Renda, *Ethics, Algorithms and Self-driving Cars–A CSI of the 'Trolley Problem,'* CEPS POL'Y INSIGHT (Ctr. for Eur. Pol'y Stud., Brussels, Belg.), Jan. 2018.

regulatory category.[168] In 2018, Democratic senators refused to pass legislation establishing a federal standard for autonomous vehicles, as they worried that the technology remains immature and underdeveloped.[169] At the state level, a majority of states have considered, but still have not enacted, rules for autonomous vehicles. Four states issued rules for testing driverless cars in public, but none address the disclosure of algorithms, nor the liability assignment for self-driving and semi-self-driving car accidents.[170] Due to the paucity of safety regulations that monitor the design and development of machine-learning algorithms, the miscalculations, misbehaviors, and malfunctions of algorithms deviating from the expectations of programmers can be difficult to correct, posing risks and injuries to the larger public as a result.

C. Information Disclosure for Public Oversight as a Solution

With the increasing frequency and magnitude of hazards associated with algorithmic opacity, machine-learning algorithms are having a major impact on firms' reputation, financial condition, and long-term development. Algorithms can also disrupt the operating results of public firms or their commercial alliances due to defects in the AI systems that firms cannot find or repair in the development process.[171] Firms involved in AI incidents may bear enormous costs and face damaging outcomes, such as lost revenues from system failures, liability to class-action lawsuits and litigation, and the destruction of reputation and shareholder value. Accordingly, firms should be required to inform corporate shareholders about material risks and incidents derived from advanced algorithms.[172] Corporate shareholders should be able to monitor firms to prevent the appearance of improper

168. *See* Andrew J. Hawkins, *Congress Takes Another Stab at Passing Self-Driving Car Legislation*, VERGE (July 28, 2019, 10:00 AM), https://www.theverge.com/2019/7/28/8931726/congress-self-driving-car-bill-redo-2019 [https://perma.cc/4H4A-M59Y] (Congress is attempting to pass new rules for driverless cars, but whether the new bill will be passed is still uncertain.).

169. Daniel Araya, *The Big Challenges in Regulating Self-Driving Cars*, FORBES (Jan. 29, 2019, 9:00 AM), https://www.forbes.com/sites/danielaraya/2019/01/29/the-challenges-with-regulating-self-driving-cars/#71e7514cb260 [https://perma.cc/5R7Z-XCVY].

170. Sebastian Blanco, *Florida Will Allow Autonomous Cars with No Safety Drivers on Public Roads Starting July 1*, CAR & DRIVER (June 18, 2019), https://www.caranddriver.com/news/a28073922/florida-autonomous-cars-driverless/ [https://perma.cc/8FE5-WUFX].

171. Sam Ransbotham, Shervin Khodabandeh, Ronny Fehling, Burt LaFountain & David Kiron, *Winning with AI: Pioneers Combine Strategy, Organizational Behavior, and Technology*, MIT SLOAN MGMT. REV. (Oct. 15, 2019), https://sloanreview.mit.edu/projects/winning-with-ai/ [https://perma.cc/37CP-QZBA] (pointing out that a growing number of AI firms perceive strategic risks from using AI technologies).

172. AUTORITÉ DE LA CONCURRENCE & BUNDESKARTELLAMT, *supra* note 2, at 77.

trading and require consideration of preventative measures in the context of AI business applications. Without disclosure requirements, corporate insiders could trade their firms' securities while hiding material, nonpublic information that concerns the concrete risks faced by firms due to algorithms. With mandatory disclosure requirements, firms could help corporate shareholders and other stakeholders understand the material impact of algorithms on firms' economic profits and sustainability.[173] Moreover, the disclosure framework would encourage firms to develop a management approach for addressing AI incidents that the firm has experienced or is likely to experience.

To address the problem of algorithmic opacity that endangers customers, investors, and other stakeholder interests, compelling information disclosure is necessary to control risks created by the operation of algorithms. As previous AI incidents have indicated, in a digital world, algorithmic opacity presents increasing risks and dangers to customers and to firms utilizing algorithms.[174] As firms increasingly rely on algorithms, society faces an evolving landscape of algorithmic threats in which algorithms penetrate individuals' lives through manipulation, invasion of privacy, and racist classification, among other ways. The threats associated with algorithmic opacity, in turn, incur a substantial risk to the financial condition of firms, the interests of shareholder benefits, the stability of capital market, and require SEC regulatory instruments to decrease the acute danger posed by advanced algorithms.

IV. SEC REGULATORY INSTRUMENTS OF INFORMATION DISCLOSURE

Although algorithmic opacity seems to be a newly debated issue, opacity as a threat to investors and modern capital markets has existed in corporations for decades.[175] Historically, mainstream public discussion has long acknowledged the risks of opacity associated with

173. Vox Creative, *How AI Can Help Us Clean Up Our Land, Air, and Water*, RECODE (Oct. 26, 2018, 11:34 AM), https://www.recode.net/ad/18027288/ai-sustainability-environment [https://perma.cc/QKZ6-WEEN] (suggesting that AI should be used to facilitate sustainability).

174. S.P. Kothari, Chief Economist & Dir., Div. of Econ. & Risk Analysis, SEC. EXCH. COMM'N, Policy Challenges and Research Opportunities in the Era of Big Data (July 13, 2019) (stating that the unpredictability of some machine-learning algorithms deployed in industries is inherently challenging for the SEC to monitor and regulate).

175. *See* Joel Seligman, *The Historical Need for a Mandatory Corporate Disclosure System*, 9 J. CORP. L. 1, 1 (1983); Frank H. Easterbrook & Daniel R. Fischel, *Mandatory Disclosure and the Protection of Investors*, 70 VA. L. REV. 669, 669 (1984); John C. Coffee, Jr., *Market Failure and the Economic Case for a Mandatory Disclosure System*, 70 VA. L. REV. 717, 722 (1984).

corporate accountability.[176] More recently, with the rise of corporate social responsibility (CSR), also termed "environmental, social and governance,"[177] corporations are increasingly required to promote social policies by disclosing information in response to social issues under corporate and securities laws.[178] In the United States, the amalgamation of disclosure obligations with public goals is evidenced by a number of regulations issued by the SEC. From the 2010 guidance on climate change disclosure to the recent conflict mineral reporting rules,[179] the SEC has established a disclosure framework that combines key elements of CSR and risk-related reporting.[180] Under the current SEC disclosure framework, several industry-specific guides have been issued for firms to fulfill its requirements.[181]

However, the SEC has not yet established any public rules that specifically address AI systems and disclosures. In this vein, a firm is not required to disclose its use of machine-learning algorithms in a timely and specific manner. Currently, very few firms are known to submit systematic and substantial algorithmic disclosures in their reports filed to the SEC. Since little attention has been paid to how firms disclose their use of algorithms under the current disclosure framework, the following Section introduces an SEC disclosure framework for public firms, discusses how it would apply to firms using AI systems, points out its practical deficiencies in addressing algorithmic opacity, and then proposes new disclosure requirements that fix the problems surrounding algorithmic opacity.

A. A Brief Introduction to the SEC Disclosure Framework

The principal purpose of the Securities Exchange Act of 1934 was to ensure public availability of reliable and adequate information about firms with publicly traded stocks.[182] To achieve this objective, the Act required a number of periodic and current reports to be filed with the SEC. All firms subject to the Act must provide disclosure through

176. For an introduction to corporate mandatory disclosure, see DAVID KERSHAW, COMPANY LAW IN CONTEXT: TEXT AND MATERIALS 13–21 (2012).

177. Corporate social responsibility refers to a business enterprise's voluntary actions to create its long-term value not only for its economic profits but also for the interests of stakeholders affected by its commercial practices or policies. *See* Marrewijk, *supra* note 32, at 102.

178. *Corporate Social Responsibility Disclosure Efforts by National Governments and Stock Exchanges*, HAUSER INST. FOR CIV. SOC'Y (Harv. Kennedy Sch., Cambridge, Mass.), Mar. 27, 2015.

179. *See* SEC Guidance on Climate Change Disclosure, *supra* note 28.

180. Business and Financial Disclosure Required by Regulation S-K, Exchange Act Release No. 34-77599, 81 Fed. Reg. 23,916 (Apr. 22, 2016).

181. *See* 17 C.F.R. §§ 229.802(a)–(g) (2018).

182. THOMAS HAZEN, THE LAW OF SECURITIES REGULATION 135 (7th ed. 2017).

annual, quarterly, and current reports.[183] When a firm is required to file a disclosure document with the SEC, the requisite form generally refers to the disclosure requirements of Regulation S-K, which lays out a disclosure framework for nonfinancial disclosure filings.[184] This, in turn, creates a set of topics, principles, and standards for mandatory disclosure. Specifically, the information provided should be clear, comparable to competitors' performance, and timely for investors to make informed decisions. Pursuant to the regulation, public firms should disclose relevant information that is likely to influence a reasonable investor when voting or making investment decisions, which is dubbed "material" information.[185] The materiality standard applies to key topics of disclosure, including business descriptions, legal proceedings, risk factors, and so forth.[186]

The current SEC disclosure framework is inadequate to address algorithmic opacity problems. Complex and opaque AI systems, particularly those built with machine-learning algorithms, can impose high informational costs on any group of stakeholders, be they investors, customers, regulators, policy makers, or the public. The invisible inner workings and applications of machine-learning algorithms pose a formidable obstacle for regulators seeking to reduce the risks entailed by algorithms. Despite this, firms' filing reports to the SEC barely describe the use of algorithms. Among those firms disclosing AI services, most only mention algorithms and their risks without providing technical and practical details. Under current practices, outsiders are not allowed to understand, surveil, or evaluate the inner workings and operating results of firms' algorithms, the substantial risks therein, and how firms are controlling those risks. Under this regulatory gap, risks derived from opaque algorithms are difficult to detect, preventing corporate shareholders and other stakeholders from monitoring firms or gaining sufficient information to make investment decisions.

183. *Id.* at 136.

184. *Id.*

185. *See* TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 446–47 (1976).

186. On August 8, 2019, the SEC proposed an amended rule for the purpose of modernizing several Items under the Regulation S-K, including the description of business, legal proceedings, and risk factor disclosures. For a detailed introduction to the SEC's recent proposal, see Gerald J. Guarcini, Franc Del Fosse & Joanna Jiang, *SEC Proposes to Modernize, Improve, and Simplify Disclosure Framework Under Regulation S-K*, NAT'L L. REV. (Aug. 15, 2019), https://www.natlawreview.com/article/sec-proposes-to-modernize-improve-and-simplify-disclosure-framework-under-regulation [https://perma.cc/4E96-7K7Y].

B. Towards an Algorithmic Disclosure Framework

After an introduction to crucial components of the SEC disclosure requirements, the Sections below outline how current practices have furthered algorithmic opacity, causing the erosion of democratic norms and damage to financial profits. Then, through the lens of the SEC disclosure framework, this Article argues for a more nuanced approach to requiring algorithmic disclosures that addresses new perils derived from algorithmic opacity.

1. Materiality Standard

Materiality is the standard that establishes what information a public firm is obligated to impart under securities laws. The basic concept of "materiality" was formulated by the US Supreme Court in *TSC Industries v. Northway, Inc.*, where the Court decided that information is material if there is a strong probability that a reasonable investor would have considered such information "as having significantly altered the 'total mix' of information available" to the public.[187] Assessing materiality requires an evaluation of all the relevant facts and circumstances at the time of reporting.[188] Firms are expected to consider both quantitative material and qualitative information,[189] as well as quantitatively small misstatements that may be considered material.[190]

Under the current disclosure framework, the SEC has not established an industry-specific materiality standard for AI systems. Firms must decide whether the expressed requirements impose an obligation to disclose certain topics. When firms prepare reports to be filed with the SEC, they must consider the materiality of risks and incidents caused by their algorithms and disclose any information that a reasonable investor might consider crucial in voting or making investment decisions. However, given the cost of disclosures and the resulting concerns about their AI services, firms have a strong motive to not disclose algorithm operations that are potentially deficient, unequal, or harmful, making the risks posed by their algorithms

187. *TSC Indus.*, 426 U.S. at 449; *see also* 17 C.F.R. §§ 240.12b-2, 240.12b-20.

188. Ganino v. Citizens Utils., 288 F.3d 154, 161–62 (2d Cir. 2000).

189. *See* SEC Staff Accounting Bulletin No. 99 (Aug. 12, 1999). *But see* Kenneth C. Fang & Brad Jacobs, *Clarifying and Protecting Materiality Standards in Financial Statements: A Review of SEC Staff Accounting Bulletin* 99, 55 BUS. LAW. 1039, 1039 (2000) (noting that historically, materiality determinations often referenced a quantitative standard).

190. SEC Staff Accounting Bulletin No. 99, *supra* note 189. *But see* Fang & Jacobs, *supra* note 189, at 1039.

difficult to detect by outsiders. Because the SEC does not specifically require algorithmic disclosure, firms can omit information that involves problematic operation of algorithms without being fined.

In addition, under the current materiality standard, firms are only obligated to consider the interests of corporate shareholders. The operating results may implicate broader concerns for the larger public that are closely connected with firms' reputation and profits and are easy to conceal from public view. Although the use of algorithms may be considered material to firms' business, firms can argue that the technicalities of algorithms are not material to a reasonable investor. In cases like that of robo-advisors, some of the technicalities of the model may be material to investors,[191] yet for other far-reaching business applications of algorithms, firms can avoid disclosure by arguing that their algorithms are immaterial to investors. As a result, under the protection of trade secrecy, crucial information on algorithmic designs and operations cannot be taken from firms and further scrutinized by corporate shareholders, resulting in no safeguard against firms developing unreliable algorithms.[192] Given the limits of the existing materiality standard that allows problematic AI business practices to escape from shareholder and public scrutiny, reforming the current disclosure standard is of immense significance.

a. Proposed Algorithmic Disclosure Considerations

Considering the nature and impacts of algorithmic opacity, this Article proposes a new materiality standard that integrates certain paramount disclosure considerations, such as stakeholder interests, sustainability, comprehensibility, and minimum necessary principles, for algorithmic disclosures.

i. Stakeholder Interests

Similar to current practices, to build an effective disclosure framework that helps control risks associated with algorithmic opacity, firms would be required to disclose clear, complete, comparable, and timely information about AI developments, operating results, and perils for investors to measure the firms' performances.

However, unlike the current materiality standard, which allows firms to determine items that may reasonably be considered important for influencing the decisions of investors, this Article argues that in

191. *IM Guidance Update*, SEC. EXCH. COMM'N (Feb. 2017), https://www.sec.gov/investment/im-guidance-2017-02.pdf [https://perma.cc/Z85Y-XH88].

192. *See supra* Section III.A.2.

algorithmic disclosure, firms should include items not only concerning the interests of their investors but also those of other stakeholders in AI systems. Stakeholders play a key role in deciding the value of AI systems, including but not limited to investors, employees, algorithm developers, suppliers, and local communities. Systematic stakeholder consideration will help strengthen algorithmic accountability across firms, corporate shareholders, and the public, decreasing dangers posed by algorithms and false suspicions against opaque applications. Hence, when determining the materiality of a topic, firms should consider the impacts of their AI services on all stakeholders and disclose information they reasonably expect. When facing conflicting expectations among stakeholders, firms are encouraged to describe how they balance them in their reports. Whenever information implicates material stakeholder concerns, it should no longer be shielded by the protection of trade secrecy and hidden from public scrutiny.

ii. Sustainability Consideration

Second, given that algorithmic opacity is causing unprecedented perils that penetrate human lives,[193] firms have a duty to develop sustainable algorithms that protect humans and their environments. Sustainability is defined as a business enterprise's creation of long-term value not only for its economic profits but also for the benefits of stakeholders affected by its commercial practices.[194] Without a sustainability consideration, not only would individuals potentially be affected, but the larger public may suffer from unexpected damage to financial profits and democratic norms. A sustainability standard would require firms to mitigate problems surrounding algorithmic opacity that implies far-reaching consequences for the larger public.[195] This element in the proposed disclosure framework encourages corporate long-term thinking and encouragement of performance in the wider context of sustainability, which is absent in the current

193. *See supra* Section III.B.

194. *See supra* note 32.

195. *See generally* Florian Möslein & Karsten Engsig Sørensen, *Nudging for Corporate Long-Termism and Sustainability? Regulatory Instruments from a Comparative and Functional Perspective*, 24 COLUM. J. EUR. L. 391 (2018); *see also* Stavros Gadinis & Amelia Miazad, *Sustainability in Corporate Law*, HARV. L. SCH. F. CORP. GOVERNANCE (Sept. 24, 2019), https://corpgov.law.harvard.edu/2019/09/24/sustainability-in-corporate-law/#:~:text=Stavros%20Gadinis%20is%20professor%20of,based%20on%20their%20recent%20paper [https://perma.cc/4QK9-CLF3].

framework.[196] In this regard, firms using machine-learning algorithms would be required to describe their strategies, risks, and goals relating to safe algorithms that benefit the larger public in the long term. Further, firms would need to describe whether and how their AI systems could create negative impacts on communities in different locations.

iii. Comprehensible Disclosure

Third, with the technical opacity involved in advanced algorithms, stakeholders cannot understand the inner workings and applications of algorithms without sufficient explanations.[197] To mitigate technical opacity, firms would need to make explanations of their AI systems comprehensible to people with all levels of expertise.[198] Using supporting reasons and illustrations, an adequate explanation should provide sufficient information that allows stakeholders to consider the operating results of machine-learning algorithms and their potential risks.[199] Adequate explanations also require firms to open a legal black box to describe the design and behaviors of AI systems for stakeholders to measure the perils generated by machine-learning algorithms.[200] Under this requirement, both technical and legal opacity will be reduced through meaningful explanations that illuminate the algorithmic design, operating process, performance, and associated risks previously hidden from public view.

---

196. *Cf.* Barnali Choudhury, *Social Disclosure*, 13 BERKELEY BUS. L.J. 183, 183 (acknowledging "a growing interest in using disclosure rules in corporate and securities law to achieve social policy goals").

197. This is also a core principle proposed by a group of researchers promoting principles (responsibility, explainability, accuracy, auditability, and fairness) for accountable algorithms. *See* Nicholas Diakopoulos, Sorelle Friedler, Marcelo Arenas, Solon Barocas, Michael Hay, Bill Howe, H.V. Jagadish, Kris Unsworth, Arnaud Sahuguet, Suresh Venkatasubramanian, Christo Wilson, Cong Yu & Bendert Zevenbergen, *Principles for Accountable Algorithms and a Social Impact Statement for Algorithms*, FAT/ML, https://www.fatml.org/resources/principles-for-accountable-algorithms [https://perma.cc/LGM5-RMBH] (last visited Oct. 3, 2020).

198. Mike Ananny & Kate Crawford, *Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application Algorithmic Accountability*, 20 NEW MEDIA & SOC'Y 1, 9 (2018) ("Learning about complex systems means not simply being able to look inside systems or take them apart. Rather, it means dynamically interacting with them in order to understand how they behave in relation to their environments.").

199. Marco Tulio Ribeiro, Sameer Singh & Carlos Guestrin, *"Why Should I Trust You?" Explaining the Predictions of Any Classifier* 1–2 (2016), https://arxiv.org/pdf/1602.04938.pdf [https://perma.cc/9UDA-6GSL]; Finale Doshi-Velez & Been Kim, *Towards A Rigorous Science of Interpretable Machine Learning* 1 (Mar. 2, 2017), https://arxiv.org/pdf/1702.08608.pdf [https://perma.cc/SH78-K36C].

200. Ribeiro, et. al., *supra* note 199; Mukherjee, *supra* note 89.

iv. Minimum Necessary Disclosure

Finally, considering the tensions between democratic transparency and commercial competition, the proposed framework requires only minimum necessary disclosure—information unnecessary for public oversight is not required, thus appropriately protecting firms' trade secrets. In this vein, this Article presents a two-layered disclosure framework. The first layer is mandatory disclosure, which consists of items that are most pertinent to producing risks. Mandatory disclosure requires firms to provide information originally protected by the legal black box because the very solution to algorithmic opacity is more knowledge—more knowledge of how firms are building and using algorithms that make decisions for humans, and more information about the perils that arise for stakeholders. Not all information has to be disclosed, but information pertaining to public interests, such as an unexpected machine-learning-algorithm malfunction occurring in a driverless car system, should be disclosed. The second layer is recommending disclosure, which includes items that firms are encouraged to disclose. For instance, firms using machine-learning-based AI systems would be encouraged but not compelled to disclose a test data set for model assessment. Recommending disclosure is a middle ground that mixes government regulation with self-regulation. In this way, costly and controversial requirements will not be imposed on firms. Firms using AI systems can choose the optimal means by which they will reach their expected goals. The two-layered disclosure framework adds flexibility and adaptability for firms to fulfill algorithmic disclosure requirements without unnecessary government intervention. Although firms are compelled to satisfy only mandatory disclosure, they are recommended to disclose additional information, particularly concerning the financial, legal, or reputational operating consequences of algorithms.

2. Disclosure Topics

The above-mentioned disclosure principles can be integrated into the existing four disclosure topics of business description, legal proceedings, risk factors, and management's discussion and analysis of financial condition and results of operations (MD&A), which are the most pertinent nonfinancial factors with respect to algorithmic disclosure. In the following discussion of these four disclosure topics, this Article first introduces the current state of regulation, including Regulation S-K and the SEC sustainability disclosures that can be used as a conceptual model for algorithmic social disclosures. Next, this

Article uses filing reports from Artificial Intelligence Technology Solutions (AITX),[201] a firm that extensively uses advanced AI systems it has developed to automate various intelligent security, concierge and operational tasks,[202] to illustrate the current practices of algorithmic disclosures under the existing regulatory framework and highlight deficiencies in disclosure. Then, this Article proposes algorithmic disclosure requirements for each of these four disclosure topics.

a. Description of Business

i. Current State of Regulation

Currently, Item 101 of Regulation S-K requires firms to describe their business development over the last five years.[203] In the disclosure documents, firms must address items such as their organizational structures, major products and services, relationships with business partners, and competitive situations.[204] In general, firms are often required to explain in detail how they generate revenue. This includes describing and distinguishing between current business activities and planned business activities. Because the nature of firms may be altered by subsequent transactions, the SEC often asks firms to provide additional essential details about their post-transaction business. Sometimes, firms are asked to provide clearer disclosure about their structure and control arrangements.[205]

With respect to sustainability disclosure, firms should disclose the compliance costs associated with enacted environmental laws. The regulation also requires a description of any predicted substantial expenses for environmental control facilities.[206] Firms must pay attention to legal, technological, and political developments relevant to climate change.[207] If any developments create challenges or

201. A.I. Tech. Sols. Inc., Annual Report (Form 10-K) 1–2 (Aug. 28, 2019) [hereinafter AITX Form 10-K]; A.I. Tech. Sols. Inc., Annual Report (Form 10-K/A, Amendment No. 1) 1–2 (Aug. 29, 2019) [hereinafter AITX Form 10-K(A1)]; A.I. Tech. Sols. Inc., Annual Report (Form 10-K/A, Amendment No. 2) 1–2 (Nov. 4, 2019) [hereinafter AITX Form 10-K(A2)].

202. AITX Form 10-K(A2), *supra* note 201, at 1.

203. 17 C.F.R. § 229.101.

204. *Id.*; *see also* Wilson v. Great Am. Indus., Inc., 661 F. Supp. 1555 (N.D.N.Y. 1987); Levine v. NL Indus., Inc., 926 F.2d 199 (2d Cir. 1991); *In re* Seagate Tech. II Sec. Litig., [1989 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 94,502 (N.D. Cal. May 3, 1989); SEC Guidance on Climate Change Disclosure, *supra* note 28, at 6293.

205. SEC Guidance on Climate Change Disclosure, *supra* note 28.

206. This requirement applies to the remaining and succeeding fiscal year as well as any further material periods. *Id.* at 6295–96.

207. *See id.* at 6296.

opportunities for firms and significantly impact their business, firms must provide further explanations.[208] For example, the SEC expects firms to explain if there is increased or decreased demand for certain products or services.[209] Firms should also disclose shifts in operating plans whenever they intend to seize new opportunities, including proposed acquisitions of equipment or plants.[210] With respect to these matters, the SEC asks firms to consider their own particular facts and circumstances in evaluating the materiality of these opportunities and obligations.[211]

ii. Current Practices and Their Deficiencies

Under current regulations, if the use of algorithms may materially influence a firm's organizational structures, major products and services, relationships with business partners, or competitive situations, the firm must provide further information on the use of algorithms. In practice, according to filing reports from AITX, disclosure of its AI service was described in very general terms.[212] AITX briefly outlined its mission of using AI technology as addressing costly and difficult problems, omitting several pieces of information that are material to stakeholders.[213] First, to fulfill that mission, it described several critical AI techniques used in its service, including "facial recognition," "cloud services," and "integrated AI software/hardware,"[214] but it did not specify the types of algorithms it used. Second, although it explained that its service employed AI-based software to simulate solutions and developed automated access control functions through facial recognition, it did not describe the unpredictability of that software.[215] Third, AITX claimed that these AI technologies helped it to outperform its competitors in its target market; however, it did not readily explain its competitive conditions, major customers, or business strategies to address changing market demands.[216] Fourth, in the description of its previous business, AITX mentioned that its first version of a commercial rugged outdoor security

208. *See id.*
209. *Id.*
210. *See id.*
211. *See id.*
212. *See* AITX Form 10-K, *supra* note 201, at 1–6; AITX Form 10-K(A2), *supra* note 201, at 14.
213. *Id.* at 1.
214. *Id.*
215. *Id.*
216. *Id.* at 5.

robot was "rejected by customers due to unsatisfactory reliability and some technical flaws that could not be solved."[217] However, AITX did not provide additional information on such flaws, and it omitted any description of the efforts to address previous flaws and how the second version of mobile robots achieved the desired outcome.[218] Instead, AITX briefly described its available software solutions by mentioning that the service "has created a variety of front-end and back-end software solutions to power their ecosystem."[219] Fifth, for manufacturing and assembly, AITX merely mentioned where it purchased raw materials, without discussing the organization for and process of building the algorithm systems.[220] Finally, regarding customer acceptance, AITX stated that its service had been used in a number of industries, including logistics, real estate, medical service, and retail industries, to emphasize its service's practicality, without further discussion of the material effects of its AI service.[221] Based on AITX's disclosure of business description, stakeholders are unable to understand any material information related to the AI system, such as the role of algorithms in its service, algorithmic design and performance, the business organization for developing algorithms, and how its AI service performs in the market.

iii. Proposed Algorithmic Disclosure Requirements

To address algorithmic opacity, effective disclosures in the description of the business must include firms' AI products and services, the institutional framework for developing a machine-learning AI system, major targeted customers, and competitive conditions. Unlike the current framework, where firms can choose not to disclose their AI systems, the proposed framework requires that whenever firms release a new product based on machine-learning algorithms, they are compelled to disclose information on that product or service. In order to help readers understand the workings of algorithms, the disclosure must explain the desired outcome of the algorithms, what types of algorithms they are using, and how those algorithms operate in selected platforms.[222] Accordingly, the design concept, crucial components, and expected outcomes of the algorithms can be understood and scrutinized by stakeholders.

---

217. *Id.* at 3.
218. *Id.*
219. *Id.* at 4.
220. *Id.*
221. *Id.* at 6.
222. Mukherjee, *supra* note 89.

In response to potential misbehaviors of algorithms that may cause inequality, injury, or even death, firms must describe the unpredictability of machine-learning algorithms. Specifically, they must adequately open the black box by explaining whether and how any machine-learning operation makes an unexpected move. If there is an unexpected move, they must explain whether that move is within the scope of their design function.[223] If the actions of an advanced AI system rely partially on experience following its programming, firms must periodically update the stability of its performance in the real world. They are encouraged to prepare a test data set for model assessment.[224]

In terms of the institutional frameworks in developing learning algorithms, firms must give stakeholders the ability to measure the sustainability and maturity of business organizations for their systems. Specifically, firms must adequately describe the interactions among the participants that build an AI system, as well as the hardware and software environments for testing the machine-learning algorithms.[225] Moreover, because the AI market is subject to rapid technological change, firms should to some extent open a commercial black box, such as updating descriptions to reflect any critical changes in post-transaction business and describe its current state of business and future strategies, considering new opportunities or risks that may materially affect demand for AI business.

b. Legal Proceedings

i. Current State of Regulation

Currently, firms must also disclose all material pending legal proceedings to which they or their subsidiaries are a party. This requirement includes the court in which any proceedings are pending, the date the proceedings are instituted, the principal parties thereto, a description of the factual basis alleged to underlie the litigation, and the relief sought. Firms are also required to disclose if a governmental entity is involved in similar investigations and litigations,[226] or if their property is the subject of a legal proceeding.[227]

---

223. Scherer, *supra* note 156, at 365 ("[A] computer chess program might make an unexpected move, but it is still not doing anything other than playing chess.").

224. TREVOR HASTIE, ROBERT TIBSHIRANI & JEROME FRIEDMAN, THE ELEMENTS OF STATISTICAL LEARNING: DATA MINING, INFERENCE, AND PREDICTION 222 (2d ed. 2009).

225. *Id.*

226. *Id.*

227. 17 C.F.R. § 229.103.

Concerning sustainability, Instruction 5 to Item 103 provides some specific requirements that apply to disclosure of certain types of environmental litigation. Firms must describe routine litigation incidental to the business under three scenarios: (1) such proceedings are material to the business condition of the firm; (2) proceedings involve potential charges that exceed 10 percent of the current assets of the firm; or (3) proceedings involve potential monetary sanctions where a governmental authority is a party.[228]

ii. Current Practices and Their Deficiencies

In its filing, AITX did disclose two legal proceedings; however, neither were concerned with issues associated with algorithms.[229] In the first proceeding, AITX stated that it was sued in a federal district court for alleged misappropriation of trade secrets through a third party.[230] However, AITX omitted several relevant pieces of information in the suit, such as the names of the principal parties, the relief sought, and detailed descriptions of the allegations.[231] In the second proceeding, AITX was sued for alleged nonpayment of fees.[232] The firm briefly described the plaintiff, the damage sought, and the resulting settlement.[233] Under current practices, where legal proceeding disclosures typically do not include substantial information on AI-related legal challenges, it is difficult for stakeholders to identify the potential problems derived from a firm's operation and estimate how existing legal proceedings might impact a firm's outlook and future financial condition.

In the era of AI, firms using algorithms to make decisions for people may face an unprecedented number of legal challenges involving competitors, law enforcement, and other regulatory agencies in the United States and beyond. As a representative example, in 2018 alone, Facebook faced numerous state and federal class actions filed against its platform and user data practices. In addition, its platform and user data practices became the subject of the FTC, the SEC, state attorneys general, and other government investigations, not only in the United

228. Commission Guidance Regarding Disclosure Related to Climate Change, *supra* note 28, at 6293.

229. AITX Form 10-K, *supra* note 201, at 14; AITX Form 10-K(A1), *supra* note 201, at 13–14; AITX Form 10-K(A2), *supra* note 201, at 14.

230. AITX Form 10-K(A2), *supra* note 201, at 14.

231. *Id.*

232. AITX Form 10-K, *supra* note 201, at 14; AITX Form 10-K(A1), *supra* note 201, at 13–14; AITX Form 10-K(A2), *supra* note 201, at 14.

233. AITX Form 10-K, *supra* note 201, at 14; AITX Form 10-K(A1), *supra* note 201, at 13–14; AITX Form 10-K(A2), *supra* note 201, at 14.

States but also in other jurisdictions, including European countries.[234] Any legal challenges could lead to changes in business practices and have a damaging impact on a firm's financial condition.[235] Legal proceeding disclosures serve as a good resource for stakeholders to understand specific misbehaviors hidden by firms under the protection of trade secrecy. Where the current disclosure framework does not require legal proceedings disclosures for algorithms, some key facts associated with the use of advanced algorithms in actions against firms may be regarded as immaterial and thus escape from stakeholders' attention.

iii. Proposed Algorithmic Disclosure Requirements

Accordingly, this Article proposes that firms provide information on the legal consequences of their machine-learning AI systems by disclosing all material pending legal proceedings associated with their AI services or products. To reduce algorithmic opacity and strengthen algorithmic accountability, firms would describe pending legal actions if their property or actions became subjects of litigation. For example, if a firm was involved in misuse of consumer data, it should report the number of complaints and lawsuits it faced associated with breaches of customer privacy, along with investigations from regulatory agencies, and the number of estimated losses of customer data. Additionally, it should provide information on the investigators or name of the court where the proceedings are pending, the interested parties in such proceedings, a description of the factual basis alleged that underlies the litigation, and the relief sought. Specifically, suppose that a firm is investigated by the FTC because the collection of information from children's online mobile devices constitutes a violation of the Children's Online Privacy Protection Act (COPPA).[236] The firm should disclose the following information: (1) how many children's information was collected; (2) the alleged fact that it collected the data from children and enabled it to disclose their personal information on their social networks without obtaining verifiable parental consent; (3) the date the matter was investigated; and (4) how the case was resolved. With the disclosure of legal proceedings, more information on problematic operating results of algorithms that may have created risks for the larger public can be discovered and monitored by stakeholders, no longer hidden from public view.

---

234. Facebook, Inc., Annual Report (Form 10-K) 30 (Jan. 31, 2019).

235. *See id.*

236. Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, §§ 1301–1308, 112 Stat. 2681 (codified as amended at 15 U.S.C. §§ 6501–6506).

c. Risk Factor

i. Current State of Regulation

Presently, Item 105 of Regulation S-K requires firms to offer a discussion of the most significant factors that make investment in the firm speculative or risky. The SEC often asks firms to describe their own risks based upon their specific facts and circumstances rather than describing risks that could apply to any firms in the industry.[237] Firms must describe the risk in a concise and organized manner and explain the impacts of the risk.[238] Past incidents involving stakeholders, such as suppliers or customers, may be necessary when crafting risk factor disclosure. Contextual disclosure should be included if it can effectively communicate risks to investors.

Concerning sustainability disclosure, firms may be required to disclose risk factors with respect to existing or pending legislation or regulation concerning climate change.[239] In risk factor disclosure, the SEC requires firms to cover all specific risks associated with climate change legislation or regulation and avoid a generic risk factor disclosure that could apply to any firm.[240] To illustrate, a firm should distinguish the nature and extent of the risks it faces in its industry from its counterparts in other industry sectors.[241] The impact of risk on a firm's reputation is another important consideration.[242] For example, based upon the nature of a firm's business and its sensitivity to public opinion, a firm may have to consider whether the public's perception of any publicly available information relating to its greenhouse gas emissions could expose the firm to potential adverse consequences to its operation due to reputation damage.[243] Also, a firm whose businesses may be vulnerable to severe weather or climate-related events should consider disclosing material risks and outcomes associated with such events in its public disclosure documents.[244]

---

237. 17 C.F.R. § 229.105.

238. *Id.*

239. *Id.*; *see* SEC Guidance on Climate Change Disclosure, *supra* note 28, at 6296–97.

240. 17 C.F.R. § 229.105; *see* SEC Guidance on Climate Change Disclosure, *supra* note 28, at 6296–97.

241. SEC Guidance on Climate Change Disclosure, *supra* note 28, at 6296–97.

242. *Id.* at 6296.

243. *Id.*

244. *Id.*

ii. Current Practices and Their Deficiencies

The disclosure reports filed by AITX barely disclosed AI-related risks in risk factor disclosure.[245] The portion that was most pertinent to AI risks concerned firms' use of data and compliance with legislation. Based on the SEC requirement, a firm must state that its AI services are in compliance with existing privacy laws and the corporate policies of clients.[246] However, AITX did not address whether privacy laws affected the development and operation of algorithms in detail, nor did it explain the specific regulations that incurred costs.[247] In addition, no information about how the firm would respond to changing legislation that may impact its AI-based service was included.

AITX briefly stated that such regulations may limit its development of AI services in its targeted market.[248] Other risks AITX noted included those that may occur in every firm, such as when it stated that "[its] success is not guaranteed and will depend on an unproven market, the efforts to rent its product, and adoption of physical security technology and their products."[249] Finally, it described several risks less relevant to algorithms, such as adversely affected intangible assets due to failure to protect intellectual property; the fact that it had "no employment agreement in place with [their] executive officers or directors;"[250] "the loss of key personnel," which could harm its business;[251] and "economic factors and financial results [that could] fluctuate and affect the future operation."[252] Despite mentioning its failure with a previous version of robot service in its business description, AITX did not mention it in its risk factor disclosure.[253] In sum, the firm omitted information about the vulnerable operation and material prior incidents it had experienced, despite admitting to the incident under other disclosure topics.[254] It is unknown how many controversial incidents have been hidden from view, how these hidden

245. *See* AITX Form 10-K, *supra* note 201, at 8–13; AITX Form 10-K(A1), *supra* note 201, at 7–13; AITX Form 10-K(A2), *supra* note 201, at 8–13.

246. *See* AITX Form 10-K, *supra* note 201, at 11; AITX Form 10-K(A2), *supra* note 201, at 11.

247. *See* AITX Form 10-K, *supra* note 201, at 11; AITX Form 10-K(A2), *supra* note 201, at 11.

248. *See* AITX Form 10-K, *supra* note 201, at 11; AITX Form 10-K(A2), *supra* note 201, at 11.

249. AITX Form 10-K, *supra* note 201, at 8; AITX Form 10-K(A2), *supra* note 201, at 8.

250. AITX Form 10-K, *supra* note 201, at 9; AITX Form 10-K(A2), *supra* note 201, at 9.

251. AITX Form 10-K, *supra* note 201, at 9; AITX Form 10-K(A2), *supra* note 201, at 9.

252. AITX Form 10-K, *supra* note 201, at 9; AITX Form 10-K(A2), *supra* note 201, at 9.

253. *See* AITX Form 10-K, *supra* note 201, at 9; AITX Form 10-K(A2), *supra* note 201, at 9.

254. *See* AITX Form 10-K, *supra* note 201, at 9; AITX Form 10-K(A2), *supra* note 201, at 9.

incidents might endanger the public, and how AITX actually mitigated the risks of such incidents.[255] Additionally, although AITX claimed that it was using several cutting-edge AI technologies, such as facial recognition, cloud service, and integrated AI software, the firm did not mention the control risks associated with advanced algorithms, including how control over advanced algorithms can be lost as they learn new data.[256] Accordingly, the risks it disclosed were too vague for stakeholders to detect flaws in the algorithms and the resulting risks. Under current practices, firms are able to conceal critical risks in their AI systems without consequence. As a result, firms can operate their AI services in a black box, trading people's safety, privacy, and equality without being challenged.

The risks posed by algorithms differ from the risks incurred by other kinds of technologies. As mentioned,[257] algorithmic opacity creates a series of problems that erode fundamental rights and endanger human safety. As the scale of risk posed by algorithms grows, an effective disclosure framework would help control risks associated with algorithmic opacity. The current disclosure framework does not specify what forms of risk are subject to disclosure, leading to firms' omissions of substantial risks posed by algorithms. To promote meaningful algorithmic disclosures, firms using machine-learning systems should take into account the potential materiality of any identified risks and offer a discussion of risk factors that make AI systems or investment in the firm speculative or risky. The impacts of AI-related incidents on firms' operating results and the public should also be considered. There are several items for firms to consider in risk factor disclosures.

iii. Proposed Algorithmic Disclosure Requirements

First, to reduce risks associated with firms' failures to respond to the changing landscape of AI regulations, the SEC should require firms to provide information on how they address risks derived from any approved or pending legislation that relates to the building of an AI system. For instance, firms using AI systems in the medical industry should consider the FDA's new guidelines on high-risk machine-learning-based AI systems.[258] Likewise, health care providers

255. *See* AITX Form 10-K, *supra* note 201, at 8–13; AITX Form 10-K(A2), *supra* note 201, at 8–13.

256. *See* AITX Form 10-K, *supra* note 201, at 8–13; AITX Form 10-K(A2), *supra* note 201, at 8–13.

257. *See supra* Section III.B.

258. Hale, *supra* note 146.

that collect data from users should describe the risks from HIPAA data privacy restrictions, which specifically prohibit unauthorized use or disclosure of protected health information.[259]

Second, there are several risks that accompany opaque machine-learning algorithms that should specifically be disclosed in detail. As mentioned before, machine-learning algorithms not only create problems of unexpectedness but also raise issues of uncontrollability. It is possible that firms could lose control of AI systems designed to learn and adapt continuously.[260] Loss of control in AI systems may thus carry a degree of risk that surpasses the risks posed by human behavior.[261] For these reasons, firms should provide explanations of risk factors in detail to inform their readers of how their systems maintain effective control of AI systems and serve the public interest.[262] When the SEC requires firms to explain the risks posed by opaque machine-learning algorithms, the public can scrutinize the inner workings and operating results of their algorithms. Meanwhile, firms will have a stronger incentive to address the risks derived from the unpredictability of algorithms to avoid being challenged by stakeholders over their AI products and services.[263]

In this regard, the SEC should require firms to consider the following issues when preparing disclosures: (1) prior AI incidents experienced by the firm that are material; (2) the severity and frequency of prior incidents, including a description of the consequences; (3) the business and organizational structure that may create material AI risks, including industry-specific risks and supply chain risks; (4) description of the ongoing risks; (5) how ongoing risks affect the firm, including the potential for reputational harm and litigation and regulatory investigation associated with AI risks; (6) the likelihood of AI incidents occurring; (7) the estimated severity of inherent AI risks; (8) the adequacy of the way the firm addresses those risks, outsources functions that contain material AI risks, and prevents such risks from reoccurring; (9) the limits of the firm's ability to reduce

259. 45 C.F.R. § 160.103. To be covered by HIPAA, firms must process and transmit protected health information in a standard HIPAA format, otherwise they are not covered entities regulated by HIPAA. SOLOVE & SCHWARTZ, *supra* note 115, at 513–14.

260. Scherer, *supra* note 156.

261. *Id.*

262. *See id.*

263. *See* WIM BARTELS, TERESA FOGELBERG, ARAB HOBALLAH & CORNELIS T. VAN DER LUGT, KPMG ET AL., CARROTS & STICKS: GLOBAL TRENDS IN SUSTAINABILITY REPORTING REGULATION AND POLICY (2016), https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/carrots-and-sticks-may-2016.pdf [https://perma.cc/3W6N-Z6BK].

AI risks; and (10) any form of undetected AI risks that may emerge in the future.[264]

Third, the SEC should require firms to disclose indirect risk concerning the impact on firms' reputations that affects firms' shareholder value. Depending on firms' reliance on reputation and vulnerability to criticism, firms may have to consider any public information concerning their AI business that may make their operating results or financial conditions suffer from reputational damage. Consider the case of Facebook: due to a series of controversies associated with its AI system—the Cambridge Analytica scandal, election-manipulating misinformation, anti-conservative bias, security breaches, and charges of privacy violations—its reputation has been severely tarnished.[265] Firms should consider this kind of reputational damage and consider whether they may run the risk of losing users, decreasing the time users spend on their service, and impacting how much users are willing to share.

Finally, under the comprehensible disclosure principle, the SEC should require firms to describe their AI risks and relevant AI incidents in context. If a firm experienced an AI incident where an unexpected algorithm malfunction occurred in its self-driving car system and caused a car to drive out of control, the firm must provide sufficient background information on this incident, including possible causes, negative consequences, and proposed solutions. Firms must provide comprehensive descriptions of AI risks to an extent that stakeholders can directly measure the risks faced by the firm. Material information regarding AI risks and incidents must be based upon firms' specific circumstances and must not be misleading. As with other management risks, the SEC should encourage firms to regularly reexamine the adequacy of their risk factor disclosure.

Given the information asymmetries accompanied by opaque algorithms that can incur widespread and cascading dangers, mapping the algorithmic disclosure framework becomes particularly necessary to open the black box. These proposed disclosure requirements will help stakeholders by preventing firms from using current disclosure requirements that fail to consider the nature of algorithmic opacity to

264. *See* SEC Statement and Guidance on Cybersecurity Disclosures, *supra* note 29.

265. Scott Rosenberg, *Facebook's Reputation Is Sinking Fast*, AXIOS (Mar. 6, 2019), https://www.axios.com/facebook-reputation-drops-axios-harris-poll-0d6c406a-4c2e-463a-af98-1748d3e0ab9a.html [https://perma.cc/TNE5-QUQ4].

control the risks, enhancing algorithmic transparency, and reducing hazards derived from opaque algorithms as a result.[266]

d. Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A)

i. Current State of Regulation

Pursuant to Item 303 of Regulation S-K, firms must disclose their financial condition, changes in financial condition, and operating results.[267] This includes disclosing their known business trends, demands, commitments, events, or uncertainties that might have a material impact on their financial condition.[268] Firms are also required to illustrate the quality of and changes in cash flows and earnings, so investors can estimate their performance and discuss how they predict their financial situation to compare to their current performance.[269]

On sustainability disclosure, Item 303 requires firms to assess whether any enacted climate change legislation or regulation is reasonably likely to materially affect the firm's financial condition or results of operations. If a certain law or regulation is pending, firms should generally presume the pending legislation or regulation will be enacted and determine whether it will affect their financial condition or operating results.[270] If there is such a possibility, then the SEC requires firms to describe that potential effect.[271] New business trends or risks associated with climate change, such as increased demand for new products or services, or decreased demand for existing products or services, may also be required to be disclosed as risk factors or in MD&A disclosure.[272]

---

266. Ananny & Crawford, *supra* note 198, at 9 (pointing out that "[t]ransparency concerns are commonly driven by a certain chain of logic: observation produces insights which create the knowledge required to govern and hold systems accountable").

267. 17 C.F.R. § 229.303.

268. *Id.*

269. 17 C.F.R. § 229.303. In the reviews of reporting reverse mergers, firms are often asked to "identify any significant elements of historical income or loss that will not continue in the company's post-transaction operations." *Id.*

270. SEC Guidance on Climate Change Disclosure, *supra* note 28, at 6296.

271. The firm would also have to consider disclosure of the difficulties, if material, involved in assessing the timing and effect of the pending legislation or regulation. *See id.*

272. *Id.*

ii. Current Practices and Their Deficiencies

In practice, AITX mentioned very little about its AI system in its MD&A.[273] Using AI-driven systems and cloud services, the firm's business operation focused on services designed to automate security tasks and solutions.[274] With respect to AI systems, AITX claimed that its solutions were provided by users' monthly subscription fees, and all elements of systems consisting of hardware and software design were owned by the firm.[275] The disclosed information offered little help in reducing algorithmic opacity that may cause damage to the firm and the public. The filing reports omitted information specifying the business trends, demands, commitment, and uncertainties of AITX's AI service, in spite of its important role in the performance of its business.[276] It is unclear how AITX made efforts to comply with regulations and prevented the occurrence of common dangers and legal concerns created by AI systems, such as denial of health care services based on discriminatory algorithms or consumer privacy invasion due to misuse of data.[277] Under current practices, stakeholders have no way to understand how AITX tailors an adequate management plan to develop accountable AI services that have enormous impacts on the its financial condition.[278] AITX's MD&A illustrates how firms can relax standards designed to protect users' privacy, equality, and safety, since they are allowed to operate their algorithms without a comprehensive consideration of corresponding legal consequences and adequate managerial approaches.

As AI becomes the private industry's focus of development and source of profits, the use of algorithms in the private sector has a great impact on firms' financial conditions. Yet, under the current disclosure framework, very few firms, if any, substantially disclose management discussion of the operating results of algorithms. Without pressure from public scrutiny, firms are less likely to establish managerial approaches that address financial problems resulting from algorithmic opacity. To incentivize firms to develop business strategies toward trustable

273. *See* AITX Form 10-K, *supra* note 201, at 18–25; AITX Form 10-K(A1), *supra* note 201, at 17–23; AITX Form 10-K(A2), *supra* note 201, at 18–25.

274. *See* AITX Form 10-K, *supra* note 201, at 19; AITX Form 10-K(A2), *supra* note 201, at 19.

275. AITX Form 10-K, *supra* note 201, at 19; AITX Form 10-K(A2), *supra* note 201, at 19.

276. AITX Form 10-K, *supra* note 201, at 8–11; AITX Form 10-K(A2), *supra* note 201, at 8–11.

277. AITX Form 10-K, *supra* note 201, at 11, 19; AITX Form 10-K(A2), *supra* note 201, at 11, 19.

278. AITX Form 10-K, *supra* note 201, at 18–19; AITX Form 10-K(A2), *supra* note 201, at 18–19.

algorithms, this Article's proposed disclosure framework would require firms to include specific algorithmic consideration in their MD&A disclosures. The SEC should require firms to consider known AI-associated trends, demands, commitments, events, or uncertainties that will have a material impact on their financial conditions. In this context, firms must consider the cost of developing AI systems, the costs of regulatory compliance, and other consequences of AI-related incidents. To encourage firms to develop AI systems with fewer threats of algorithmic opacity, the SEC should require firms to provide necessary management plans and information on the results of operations with far-reaching impacts on their financial conditions.

iii. Proposed Algorithmic Disclosure Requirements

First, firms would need to describe their data management plan, not only because of data's significant role in creating efficient and legitimate algorithmic applications but also because of the complex privacy regulatory landscape and the growing number of costly legal proceedings associated with misuse of data.[279] With respect to the data management plan, firms would need to disclose how they collect, develop, manage, and utilize data for AI-relevant services. Because many violations begin with incidents caused by employees unaware of privacy regulations,[280] firms would need to mention their approach to ensuring the protection of customer privacy, including how they secure customer data, educate employees, and adopt measures to protect data they obtain, process, or transfer.[281] Firms would also need to describe whether and how they use customer information for any other purposes, as well as how they communicate changes in their privacy policy to customers.

Second, firms would need to disclose their management approach to building nondiscriminatory AI systems. Given that the opaque application of algorithms replicates inequality or misrepresents the public,[282] algorithmic opacity can lead to illegitimate decision-making processes that encroach on fundamental rights and erode trust in firms using such algorithms. Although reducing bias has

279. *See supra* Sections III.B.1, III.C.

280. For the US system of consumer data privacy regulation, see SOLOVE & SCHWARTZ, *supra* note 115, at 786–90.

281. *See id.* at 533 ("Many of the FTC resolution agreements involving monetary settlements and fines began with an incident. Some of these incidents were caused by one employee or small group of employees. . . . An incident can spark an investigation by HHS, and this investigation can uncover more than just the particular violation that led to the incident.").

282. *See supra* Section III.B.2.

become a general expectation of socially responsible conduct in today's society, particularly the one after COVID-19 that aims at mitigating systematic discrimination,[283] the current disclosure framework barely considers the surrounding impact of discrimination on firms' financial conditions. To reduce the inequality hidden in algorithms, this Article's proposed disclosure framework would require firms to disclose discrimination impact assessments that include incidents associated with discrimination and describe their preventive measures against discrimination.[284] Specifically, they must provide information hidden from the public, such as how they select raw data, ensure equality when developing algorithms, and apply algorithms in business applications that have decision-making power regarding people's employment, promotion, access to medical systems, and so forth. Accordingly, they would be required to make an effort to promote equality in the applications of algorithms, as firms can no longer conceal their managerial approaches to algorithms from stakeholders.[285]

Third, safety is a desirable goal of AI applications that must be explained by firms because the existence of algorithmic opacity inevitably hinders adequate surveillance of safe AI systems. As AI products and services are expected to complete their tasks safely, firms would be required to provide information on the safeness of their AI systems, which is absent from today's disclosure framework. To ensure that firms provide a safe AI system, the proposed framework requires firms to consider safety's impact on their algorithm applications.[286] Specifically, firms would need to report percentages of machine-learning-based products and services for which safety impacts are assessed for improvement. They would also need to disclose the number of incidents derived from breaching safety regulations (e.g., driverless cars). For firms whose businesses are likely to cause safety concerns or are especially vulnerable to severe AI incidents, such as the autonomous vehicle industry, they must disclose an estimated risk control and effectiveness report in the risk factor disclosure that

283. *See Address 'Appalling Impact' of COVID-19 on Minorities, UN Rights Chief Urges*, UN NEWS (June 2, 2020), https://news.un.org/en/story/2020/06/1065272 [https://perma.cc/4CC3-6B6M].

284. The impact assessment is originated from environmental law and recently promoted by several scholars, see Katyal, *supra* note 3, at 111–17. For a discussion of impact statements in policing, see Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109 (2017).

285. *See generally* IAN AYRES, CARROTS AND STICKS: UNLOCK THE POWER OF INCENTIVES TO GET THINGS DONE (2010).

286. *See* Katyal, *supra* note 3, at 110–17; *see also* Josephine Wolff, *How to Improve Cybersecurity for Artificial Intelligence*, BROOKINGS INST. (June 9, 2020), https://www.brookings.edu/research/how-to-improve-cybersecurity-for-artificial-intelligence/ [https://perma.cc/C64Y-T6L2].

explains how they test their products or services using machine-learning algorithms to ensure the safety of both users and developers.

Fourth, in addition to the management plans and impact reports mentioned above, other aspects that may influence financial conditions are still hidden from public scrutiny due to trade secret protection. For instance, successful adoption of machine-learning systems requires high levels of expertise, which can become a substantial impediment to firm managers without adequate levels of expertise in evaluating the risks of machine-learning systems. The SEC should therefore require firms to disclose how they reevaluate and rebuild their strategic alliances and business models in response to machine-learning systems, including hiring algorithm scientists and collaborating with alliances to develop application solutions and how they posit themselves in their broader AI business ecosystem.[287]

Fifth, because corporate mergers or acquisitions often involve a significant degree of risk or effect on firms' long-term development, the SEC should require firms to disclose relevant acquisitions, mergers, intellectual capital, and other concerns emergent in the AI community, and how relevant changes in the organization affect their financial operation and future position in the burgeoning AI market.[288]

Sixth, the SEC should require firms to be transparent about the quality of and changes in AI-related earnings and cash flows for investors to more accurately measure their financial situation and estimate their future performance. In addition to disclosing material transaction activities like reverse mergers,[289] the SEC may ask firms to describe any substantial AI-caused income or loss that does not extend to their post-transaction operations. In addition, the SEC should encourage firms to pay attention to any other costs or consequences associated with risk that are reasonably likely to affect the firm's

287. *See* Michael Ehret & Jochen Wirtz, *Unlocking Value from Machines: Business Models and the Industrial Internet of Things*, 33 J. MKTG. MGMT. 111, 115–25 (2016) (using entrepreneurship and transaction cost theories to examine business models for the IoT techniques and how to further transform risks into commercial opportunities).

288. For instance, in 2018, Apple acquired Silk Labs, Oracle acquired DataFox, Microsoft made five acquisitions that included XOXOCO and Lobe. Some of them disclosed the terms of deals, while most of them acquired for an undisclosed amount. *30 Major Technology Acquisitions in 2018*, EURIUN TECHS. (Dec. 27, 2018), https://www.euriun.com/tech/30-major-technology-acquisitions-2018/ [https://perma.cc/VX6S-46NV]; Mikey Campbell, *Apple Reportedly Acquires AI Startup Silk Labs*, APPLEINSIDER, https://appleinsider.com/articles/18/11/21/apple-reportedly-acquires-ai-startup-silk-labs [https://perma.cc/5NLC-VV9L] (last visited Oct. 4, 2020).

289. According to the SEC, a reverse merger is a transaction where a private firm acquires a public reporting company to go public and obtain its access to funding in the capital markets. *See* SEC. EXCH. COMM'N, INVESTOR BULLETIN: REVERSE MERGERS 1 (June 9, 2011), https://www.sec.gov/investor/alerts/reversemergers.pdf [https://perma.cc/JNX4-4EBK].

operating results or financial condition and disclose how likely it is that this AI risk will lead to increased protection expenditures[290] or reduced revenues.[291]

Seventh, the SEC should require firms to evaluate whether any legislation will likely exert a substantial impact on their financial situation or operating results. For example, under the proposed disclosure framework, firms would need to consider legislation and regulations that may limit the use of AI systems and cause associated costs or litigation threats to firms. In terms of the cost of regulation compliance, firms would need to disclose all pending or enacted regulations that may affect their building of AI systems, including regulations and legislation on information privacy, civil laws, and cross-border rules that apply to their systems.[292] Last but not least, firms would also need to include new business trends or risks associated with AI in risk factors or MD&A disclosure.

In sum, to encourage firms to develop accountable algorithms that further consumer interests and human welfare in the long term, a disclosure system that sheds more light on harmful algorithmic opacity is necessary. Such disclosure requirements should not only concern technical information associated with AI systems but also the interactions of AI systems and stakeholders. Without new guidance on algorithmic disclosures, the SEC's materiality standard is so general and ambiguous that firms are not obligated to disclose much critical information relevant to AI risks. Because no existing disclosure requirement explicitly refers to algorithms and AI systems, firms have considerable freedom to disclose only those facts that are favorable to

290. As protection costs increase, it may bring about organizational changes, additional staff training, an increased protection scheme, expert engagement, legal proceedings, and compliance costs. *See* R. Douglas Harmon, *Cybersecurity Disclosure Heats Up*, LEXOLOGY (Apr. 4, 2014), https://www.lexology.com/library/detail.aspx?g=dbedee7c-4936-42be-be45-9da94877d104 [https://perma.cc/SZU6-QGZM]. Also, following an incident, firms have to bear remediation costs to rebuild their goodwill and attract customers to continue business relationships. *See Global Cyber Executive Briefing*, DELOITTE: INSIGHTS, https://www2.deloitte.com/gz/en/pages/risk/articles/Global-Cyber-Briefing.html [https://perma.cc/7FNL-VAU5].

291. Lost revenue may be caused by misuse of data or the loss of customers after an incident, legal proceedings, reputation damage, and the loss of competitive advantage. *See Global Cyber Executive Briefing*, *supra* note 290. Firms in an industry vulnerable to AI incidents should disclose the description of relevant insurance coverage and the cost of maintaining insurance in response to potential loss of revenue. *See generally* Ram Shankar Siva Kumar & Frank Nagle, *The Case for AI Insurance*, HARV. BUS. REV. (Apr. 29, 2020), https://hbr.org/2020/04/the-case-for-ai-insurance [https://perma.cc/7YJ5-LRKE].

292. The disclosure of any material estimated capital expenditures for AI control facilities for its remaining and succeeding fiscal year are to be covered by the MD&A disclosure. *See* 17 C.F.R. § 229.303(a)(2); SEC Statement and Guidance on Cybersecurity Disclosures, *supra* note 29, at 8170.

their business, leaving the most problematic operations out of public view. As analyzed previously, current filing reports demonstrate firms' reluctance to disclose substantial information on algorithmic matters and resistance to disclosing relevant risks and incidents.[293] With legal and technical opacity inherent in their algorithms, the law allows firms to conceal algorithmic information in detail, although the risks of algorithms may be considered material to firms' businesses and to the public. To mitigate algorithmic opacity, this Article's proposed algorithmic disclosure requirements under the SEC disclosure framework imposes obligations to disclose AI items. With obligations to disclose, the technicalities and commercial applications of algorithms can be scrutinized by stakeholders for risks. As a result, these risks to the larger public and firms themselves will be identified, controlled, and mitigated in due course.

V. LIMITATIONS, POSSIBILITIES, AND IMPACTS OF THE PROPOSED DISCLOSURE FRAMEWORK

In an era where AI firms dominate the development of algorithms, accountable AI products and services are possible if specific corners of commercial practices can be examined and monitored. As the scale of risks posed by algorithms is no less serious than that posed by previous technologies, this Article proposes a new disclosure framework for AI systems through the lens of the SEC's disclosure framework. This framework considers the technical traits of algorithms, potential dangers of AI systems, and regulatory governance systems in light of increasing AI incidents. In the previous Sections, the proposed framework addresses both opacity resulting from intentional operations aimed at hiding certain information that may adversely affect financial profits and opacity resulting from unintentional operations due to the complexities of algorithms' technical attributes. From a theoretical perspective, however, there are some limitations with this new disclosure framework—the SEC may not have the authority to regulate AI firms' behaviors, the proposed disclosures may remain uncertain direct practicability, and the disclosure requirements can be inherent in high costs.

First, one may argue that while the SEC has broad power to protect the investing public, it may not have the authority to require firms using AI systems to take into account the benefit of stakeholders other than corporate shareholders. In addition, one may question

293. AITX Form 10-K, *supra* note 201, at 18–25; AITX Form 10-K(A1), *supra* note 201, at 17–23; AITX Form 10-K(A2), *supra* note 201, at 18–25.

whether the SEC has the power to make firms disclose information that may reveal their trade secrets. Second, even if the SEC has the power to regulate algorithmic disclosure, disclosed information may be downplayed, and firms may focus on legitimate details of their use of AI systems to bolster their reputation and avoid criticism.[294] Meanwhile, given that the proposed disclosure framework only applies to public firms, firms using AI systems can avoid the SEC disclosure requirements by choosing not to go public and staying private, and continue to operate their AI systems in opacity. Third, even if the SEC can ensure that disclosure requirements applying to public firms will produce useful information, disclosure itself does not absolutely guarantee good behavior.[295] Fourth, despite recognition of positive impacts on disclosures, one may argue that the compliance cost for the disclosure requirement is too high, or that the practicability of disclosure is uncertain.[296]

Despite such potential limits, this proposal opens up more possibilities to regulate algorithmic opacity for several reasons. First,[297] the SEC has substantive power to enact disclosure rules and reshape the monitoring rules for firms using AI systems. Corporate shareholders also need sufficient information to evaluate firms' performance and outlook when making investment decisions. Algorithmic disclosure requirements allow them to make sound judgments by discerning risks and comparing firms' managerial approaches to developing and using advanced algorithms. The broader sustainability disclosure requirements enacted by the SEC, which exist for more than solely the investing public, also justify the proposed algorithmic sustainability disclosures benefiting more than just corporate shareholders. Additionally, rather than asking firms to disclose an indeterminate amount of information on their trade secrets, the proposed algorithmic disclosures, like the existing SEC cybersecurity disclosures, should not jeopardize the core secrecy of commercially valuable information and should only require minimum necessary disclosures that concern the best practices and the problematic use of their AI systems. Firms might also need a regime that gives the SEC discretion to enter their private areas because such

294. *See* Rüdiger Hahn & Regina Lülfs, *Legitimizing Negative Aspects in GRI-Oriented Sustainability Reporting: A Qualitative Analysis of Corporate Disclosure Strategies*, 123 J. BUS. ETHICS 401, 409–13 (2013).

295. *See* Stephen M. Bainbridge, *Mandatory Disclosure: A Behavioral Analysis*, 68 U. CIN. L. REV. 1023, 1023–24 (2000).

296. *See* David M. Lynn, *The Dodd-Frank Act's Specialized Corporate Disclosure: Using the Securities Laws to Address Public Policy Issues*, 6 J. BUS. & TECH. L. 327, 330–31, 335–36 (2011).

297. *See supra* Part I, Section IV.A.

authority reduces the likelihood that stakeholder concerns or government sanctions will be imposed based on false and unverifiable suspicions.

Second, even if the information firms provide may be marginalized, it provides more clues for stakeholders to monitor AI firms. Firms using machine-learning algorithms would be required, as a condition of fulfilling disclosure obligations, to allow the SEC to open the black box for stakeholder inspection. As a result, such disclosed information serves as a valuable resource for the public to investigate firms' AI systems. If information can be drawn from firms, those firms will have to specify how they build reliable AI products and services from the very start. By doing so, firms are more likely to develop accountable algorithms and AI systems. Even if the SEC disclosure requirements do not apply to private firms, the proposed algorithmic disclosure framework is a workable first step that applies to at least a large portion of industry actors to reduce algorithmic opacity. With a robust algorithmic disclosure framework, the SEC can measure its advantages and shortcomings and further decide when and how to extend algorithmic disclosures to private firms. Thus, the proposed disclosure framework can help establish a more well-rounded disclosure and transparency standard for the private sector.

Third, although disclosures do not guarantee good algorithmic behavior, they will incentivize firms to develop accountable algorithms. If the law requires algorithmic disclosures, firms will have a substantial incentive to restructure their environments to monitor the operating results and develop sustainable strategic management of their machine-learning algorithms. Because disclosure makes it easier for the public to detect firms' illegal or unethical behaviors and compare their performances, firms will face more surveillance and strive harder to reach public standards in a competitive AI market. To avoid liability and risking their reputation, firms will avoid behaviors that pose risks to the larger public. Additionally, with the obligation of disclosure toward safe algorithms, firms will have a strong motive to develop value-enhancing algorithms.[298] This is also consistent with what scholars have recently suggested—that the greatest source of transformation of AI systems are firms' efforts to develop algorithms that integrate democratic principles with a machine-learning model.[299] In this vein, the law will not be the only factor that regulates firms. Algorithmic design will work hand-in-hand with democratic rules. Such

298. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999).

299. For an analysis of Katyal's suggestions for codes of conduct, see Katyal, *supra* note 3, at 108–11.

a regulatory incentive will be useful to overcome the resistance of firms to disclose their use of algorithms under the protection of trade secrecy.

Fourth, disclosure requirements will incur costs to firms, but firms will profit if they develop stable, safe, and qualified AI services and products. Additionally, financial profits should be subordinate to public concerns, especially in the new generation of AI perils. Recently, even California, the most innovative economy in the United States,[300] has imposed burdensome privacy rules that require disclosure obligations despite strong industry opposition.[301] Only through such algorithmic disclosure requirements will firms think critically about streamlining the process of developing accountable algorithms, finding an efficient way to meet disclosure obligations. The government should provide funding to help start-ups create accountable algorithms and comply with increased disclosure burdens, which will benefit every participant in society. Disclosure requirements will also significantly reduce the cost to the government of monitoring firms that operate machine-learning algorithms.

Fifth, the proposed disclosure framework is an ideal regulatory approach that creates a twilight zone between pure legal regulation and complete self-regulation. Given the reluctance of government to enact legislation that materially regulates the development and application of algorithms, disclosure requirements provide firms with more freedom of choice. The SEC has the power to require and encourage disclosure obligations, while firms can define how to build a sustainable and accountable AI system and choose the means that best suit their specific circumstances to achieve regulatory goals. This regulatory approach is less coercive and more cost-effective than direct controls.

Sixth, this proposal attempts to strike a balance between stakeholders' interests in disclosure and firms' interests in trade secrecy. On the one hand, given the increasing frequency and magnitude of AI incidents, the proposed disclosure framework requires firms to include additional algorithmic disclosure, especially in their description of risk factors. On the other hand, to ease firms' burdens from disclosure requirements, the redesigned disclosure framework presents a scaled disclosure obligation that compels minimum

300. Shelly Hagan & Wei Lu, *California Is the Most Innovative Economy in America*, BLOOMBERG (Apr. 16, 2019, 9:11 PM), https://www.bloombergquint.com/business/california-is-no-1-massachusetts-no-2-in-u-s-innovation-rank [https://perma.cc/DZG5-7YTS].

301. *See* Tony Romm, *California Adopted the Country's First Major Consumer Privacy Law. Now, Silicon Valley Is Trying to Rewrite It*, WASH. POST (Sept. 3, 2019, 10:26 AM), https://www.washingtonpost.com/technology/2019/09/02/california-adopted-countrys-first-major-consumer-privacy-law-now-silicon-valley-is-trying-rewrite-it/ [https://perma.cc/52FY-G855].

necessary disclosure.[302] The proposed framework does not intend to require mandatory disclosure of low-risk AI systems, such as those designed to perform simple routine tasks.[303] Instead, this framework only requires disclosures of higher-risk AI systems in the private sector—those employing machine-learning algorithms whose opacity may lead to risks to stakeholders.[304] By doing so, the proposed regulatory strategy attempts to avoid the risk of imposing unreasonably burdensome, intrusive, or costly disclosure requirements.

Given the limitations and possibilities of the proposed algorithmic disclosure framework, the new requirements have a profound impact on firms' managerial approaches to developing and using algorithms, as the proposed framework will showcase firms' behaviors by requiring descriptions of data used for decision-making, the computational environment utilized, and the context of the algorithmic design and deployment. Under the proposed disclosure framework, firms will produce technical explanations that explain the complex techniques inherent in machine-learning algorithms, disclose selective information about the inner workings of algorithms that have been previously claimed as trade secrets, and facilitate social dialogue between firms and stakeholders.[305] Through disclosures of business descriptions, legal proceedings, risk factors, and MD&A, technical opacity will be reduced because firms are required to illustrate the functions, features, and unpredictability of their AI systems in understandable language under their business description disclosure requirements. Legal opacity will be eased because, in the business description disclosure, firms must disclose the inner workings of algorithms and will thus have a motive to manage all participants and components in a project to ensure that algorithms are accountable. The dangers of algorithmic opacity will be better controlled as firms must consider preventative measures and report unexpected changes in risk factors and MD&A disclosure. Risks will thus be identified early on because much more information will be disclosed for necessary assessment.

---

302. By doing so, it prevents overregulation that stifles innovation in the private sector. *See* LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY 199 (2004).

303. *See generally* Frank Säuberlich & Danko Nikolić, *AI Without Machine Learning*, TERADATA (Feb. 26, 2018), https://www.teradata.com/Blogs/AI-without-machine-learning [https://perma.cc/R84Z-CHJG] (illustrating the type of AI systems that do not rely on machine-learning-based algorithms).

304. The FDA plans to adopt a similar approach to regulate AI medical service. *See* Hale, *supra* note 146.

305. *See supra* Section III.A.

VI. CONCLUSION

In the age of AI, opacity is one of the greatest perils facing humans today. No one put it better than Justice Louis Brandeis when he said that "[s]unlight is . . . the best of disinfectants; electric light the most efficient policeman."[306] It may not be possible to stop firms' domination in developing algorithms in the next century, but it is crucial to ensure that algorithms are harmless by requiring more transparency to mitigate algorithmic opacity. It is not too late to prevent the private sector's invisible hand from making wrong or illegitimate decisions for citizens, if light can guide firms in the right direction at the proper time. With the emerging risks of algorithmic opacity, corporations need to bear the responsibility of disclosing information in ways that benefit not just corporate shareholders, but society as a whole. As firms increasingly acquire and develop machine-learning systems in support of their operations, they should have a duty to disclose in a manner that ensures interpretability, explanation, and transparency.[307]

The representative case of Facebook has shown the enormous damage caused by algorithmic opacity to users, investors, citizens, firms, the capital market, and society—and the recorded incidents are just the tip of the iceberg. Although AI incidents are growing at an unprecedented scale, few, if any, legal regimes require firms to engage in social disclosure of their algorithms. A disclosure framework that defines accountable corporate governance has moved forward, but the emerging economies shaped by algorithms are invited to embrace the existence of algorithmic opacity.

This Article has explored the impacts, possibilities, and limits of using a disclosure framework under corporate securities law to reduce opacity in privately owned AI systems. Despite its limitations, the proposed disclosure framework can be used as a model to ensure that the operations of machine-learning AI systems are explained and monitored. By adopting such a regulatory approach, firms will be incentivized to address issues surrounding algorithmic opacity, develop algorithms that protect democratic norms in society, consider the interests of corporate shareholders, and promote broader alignment of capital markets with the goal of accountability in the age of AI.

306. LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 92 (1914) ("Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.").

307. *See* Mary Lee Kennedy, ASS'N RSCH. LIBRS., RESEARCH LIBRARY ISSUES RLI 299: ETHICS OF ARTIFICIAL INTELLIGENCE 31–32 (2019), https://publications.arl.org/rli299/ [https://perma.cc/K3JE-EQVX].

Accordingly, such an algorithmic disclosure framework can help enhance transparency and promote compliance with the law and democratic standards for advanced AI systems to reduce the risks posed to stakeholders, stabilize capital markets, and promote sustainability in the long run.