# The Right to Know Social Media Algorithms

Haochen Sun*

ABSTRACT

*One of the most important legal issues in the age of social media is how to tackle algorithmic secrecy. Social media algorithms permeate society, yet most are developed and applied in a black-box manner with a range of serious social consequences. For example, the amplification of fake news by social media algorithms has caused tremendous harm to democratic governance and undermined pandemic relief measures.*

*In addressing the problems of algorithmic secrecy, the legal protection of social media algorithms as trade secrets is a major obstacle. This article explores the possibility of recognizing a right to know algorithms as the legal basis for requiring proportionate disclosure of trade secrets pertaining to social media algorithms. This new legal right would promote algorithmic transparency in the public interest.*

*The right to know, a civil liberty that enables citizens to obtain information held by the government and certain private entities, lends strong policy support to recognition of the right to know social media algorithms. As the article shows, this new right would function to protect democratic participation, public safety, and social equality, the three kinds of public interest that are of crucial importance in the algorithmic society.*

*The article then discusses how this new legal right could prevail over the trade secret protection of social media algorithms, paving the way to a multi-stakeholder approach to regulating algorithmic secrecy. This new approach would empower the legislature, administration, and judiciary to determine how social media companies should effect proportionate disclosure of information on their algorithms. Its primary aim is to promote transparency of social media algorithms, to make them more intelligible, and to hold social media companies accountable should they fail to fulfil their disclosure responsibility.*

* Professor of Law, University of Hong Kong Faculty of Law. I presented an earlier draft of this article at the Regulating Social Media Algorithm conference, the Explainable AI Workshop, the Law and Technology Consortium conference, and the 2023 Intellectual Property Scholars Conference. I am grateful to the participants at these events for their feedback and also to Anupam Chander, Danielle Citron, Xiaodong Ding, Jeanne Fromer, Woodrow Hartzog, Sonia Katyal, Lyria Bennett Moses, Frank Pasquale, Pamela Samuelson, and Christopher Yoo for their helpful conversations and comments.

> "The choice of which algorithm to use (or not) should be open to everyone."
>
> —Jack Dorsey, Former Twitter CEO †

> "Too often, Big Tech's algorithms put profits before people, from negatively impacting young people's mental health, to discriminating against people based on race, ethnicity, or gender, and everything in between."
>
> —Senator Tammy Baldwin ‡

---

† Rachel Metz, *Elon Musk Thinks Twitter's Algorithm Should Be Public. Here's What That Could Mean*, CNN (Apr. 19, 2022), https://edition.cnn.com/2022/04/19/tech/twitter-algorithm-open-source-elon-musk/index.html [https://perma.cc/R34S-7CDV].

‡ Press Release, *Wyden Booker and Clarke Introduce Algorithmic Accountability Act of 2022 to Require New Transparency and Accountability for Automated Decision Systems* (Feb. 3, 2022), https://www.wyden.senate.gov/news/press-releases/wyden-booker-and-clarke-introduce-algorithmic-accountability-act-of-2022-to-require-new-transparency-and-accountability-for-automated-decision-systems [https://perma.cc/5JBY-48EA].

## INTRODUCTION

What legal right matters most in an algorithmic society? Algorithms are radically transforming the ways in which we experience our world, mak- ing this a legal and policy question of utmost urgency.[1] They also control ev- ery single aspect of our social media lives. They dictate what we see, read, and hear on social media[2] and determine how our personal data are collected and utilized.[3] But despite their pervasiveness and potency, the ways in which social media algorithms function to monitor and influence our behaviors are largely unknown to us.

In the algorithmic society, a legal right to know about the workings of social media algorithms is of utmost importance, yet no such right exists. Instead, social media algorithms are developed, applied, and even legally protected as black boxes.

To a significant degree, the law safeguards our legal right to be informed about risks associated with our consumption of life's necessities. Regulations require producers of food and medicines, for example, to supply consumers with basic information about ingredients and to disclose any potential side effects.[4] This protection of consumers' right to know enables the making of informed decisions.

In stark contrast, our consumption of social media takes place in an environment that is unregulated and opaque, rife with political polarization,

---

[1] For the concept of "algorithmic society," *see* Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1151 (2018) [hereinafter Balkin, *Free Speech in the Algorithmic Society*] ("the Algorithmic Society . . . features large, multinational social media platforms that sit between traditional nation states and ordinary individuals, and the use of algorithms and artificial intelligence agents to govern populations."); Jack M. Balkin, *Free Speech Versus the First Amendment* 8 (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4413721 ("[W]e are now well into what I have called the Algorithmic Society, a world in which more and more public and private decision making and governance occurs through the use of algorithms, automated decision systems, artificial intelligence, and data science."); THE ALGORITHMIC SOCIETY: TECHNOLOGY, POWER, AND KNOWLEDGE 1 (Marc Schuilenburg & Rik Peeters eds., 2020) ("We live in an algorithmic society. Algorithms have become the main mediator through which power is enacted in our society.").

[2] *See* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1603 (2018) (arguing that "platforms should be thought of as operating as the New Governors of online speech"); Evelyn Douek, *Contend Moderation as Systematic Thinking,* 136 HARV. L. REV. 526, 530 (2022) (discussing the mass speech administration role played by social media platforms).

[3] *See* ALFRED R. COWGER JR., THE THREATS OF ALGORITHMS AND AI TO CIVIL RIGHTS, LEGAL REMEDIES, AND AMERICAN JURISPRUDENCE: ONE NATION UNDER ALGORITHMS 65, 102-03 (2020).

[4] *See, e.g.*, U.S. Food & Drug Administration, *What We Do*, https://www.fda.gov/about-fda/what-we-do [https://perma.cc/EG8C-493Q] ("FDA is responsible for advancing the public health by helping to speed innovations that make medical products more effective, safer, and more affordable and by helping the public get the accurate, science-based *information* they need to use medical products and foods to maintain and improve their health.").

misinformation, and discrimination.[5] Harmful speech swirling on Facebook is said to have swayed the outcome of the 2016 U.S. presidential election[6] and to have triggered the 2021 Capitol attack.[7] Amid pervasive disinformation on social media, the World Health Organization declared the COVID-19 pandemic an "infodemic"[8] that had caused mental distress, bred mistrust in health authorities, and undermined pandemic relief measures.[9] The secrecy of social media algorithms threatens other crucial public interests, too, such as national security[10] and racial equality.[11]

In response to growing problems with algorithmic secrecy, this article argues that people should be bestowed with a new legal right to know about the workings of social media algorithms. This right has not been conjured out of thin air. Rather, it is derived from the right to know, a full-fledged civil liberty protected by international human rights treaties such as the Universal Declaration on Human Rights and domestic laws such as the U.S. Freedom of Information Act.[12] The right to know prevents the government and certain private entities from concealing critical information on the decisions they make, thereby providing citizens with a means of acquiring knowledge on such decisions.[13] In this article, I propose that the right to know should be

---

[5] FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 216-17 (2016) (arguing that "the wholesale use of black box modeling, however profitable it is for the insiders who manage it, is dangerous to society as a whole").

[6] Danielle Kurtzleben, *Did Fake News on Facebook Help Elect Trump? Here's What We Know*, NPR (Apr. 11, 2018), https://www.npr.org/2018/04/11/601323233/6-facts-we-know-about-fake-news-in-the-2016-election [https://perma.cc/AK9X-VWY2].

[7] Craig Timberg et al., *Inside Facebook, Jan. 6 Violence Fueled Anger, Regret over Missed Warning Signs*, WASH. POST (Oct. 22, 2021), https://www.washingtonpost.com/technology/2021/10/22/jan-6-capitol-riot-facebook [https://perma.cc/32PL-3PNM].

[8] *Infodemic*, WORLD HEALTH ORG., https://www.who.int/health-topics/infodemic#tab=tab_1 [https://perma.cc/FE5F-MVHE ] (last visited Feb. 28, 2023).

[9] *See* Michael A. Gisondi et al., *A Deadly Infodemic: Social Media and the Power of COVID-19 Misinformation*, 24 J. MED. INTERNET RES. e35552 (2022).

[10] *See* Steven Lee Myers & Eileen Sullivan, *Disinformation Has Become Another Untouchable Problem in Washington*, N.Y. TIMES ( July 6, 2022), https://www.nytimes.com/2022/07/06/business/disinformation-board-dc.html [https://perma.cc/48ZT-HKYG ] ("The Department of Homeland Security added the threat of false information to its periodic national terrorism advisory bulletins for the first time in February."); Danielle K. Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753, 1783-84 (2019).

[11] *See generally* Juyoun Han et al., *Medical Algorithms Lack Compassion: How Race-Based Medicine Impacted the Rights of Incarcerated Individuals Seeking Compassionate Release During COVID-19*, 26 STAN. TECH. L. REV. 43 (2023); Anupam Chander, *The Racist Algorithm?*, 115 MICH. L. REV. 1023 (2017); Deborah Hellman, *Measuring Algorithmic Fairness*, 106 VA. L. REV. 811 (2020); Thomas B. Nachbar, *Algorithmic Fairness, Algorithmic Discrimination*, 48 FLA. ST. U. L. REV. 509 (2021).

[12] *See infra* Part II.A.1. *See also* David C. Vladeck, *Information Access—Surveying the Current Legal Landscape of Federal Right-to-Know Laws*, 86 TEX. L. REV. 1787, 1787-88 (2008); Barry Sullivan, *FOIA and the First Amendment: Representative Democracy and the People's Elusive Right to Know*, 72 MD. L. REV. 1, 11-12 (2012).

[13] *Id. See also Open Meeting Statutes: The Press Fights for the Right to Know*, 75 HARV. L. REV. 1199, 1204 (1962) (showing that the advocates of the right to know sought to promote the

expanded to prevent social media companies from concealing critical information on how their algorithms affect public interests. Such expansion would confer upon citizens the right to know social media algorithms, empowering them to access and acquire knowledge on how these algorithms affect their interests as individuals and as members of society.

A major legal hurdle to achieving algorithmic transparency arises from intellectual property (IP) law and its protection of algorithms as trade secrets, which legally entitles social media companies to maintain the secrecy of their algorithms.[14] The enormous commercial value of social media algorithms makes their trade secret protection extremely important. In the past, the Coca-Cola formula was the world's most valuable trade secret;[15] today, it is Google's search algorithm.[16] In this context, at stake is whether and how the right to know social media algorithms would diminish the commercial value of businesses sustained by social media algorithms.

In this article, I will discuss how we should deal with this essential conflict between the public interest in algorithmic transparency and the private interest in algorithmic secrecy. In doing so, I suggest that the right to know social media algorithms offers two new perspectives on resolving this conflict.

First, this proposed legal right aims to enhance our understanding of the nature and scope of the public interest implicated in algorithmic transparency. I will illustrate that the right to know safeguards a range of public interests, including democratic participation, public safety, and social equality, which should be upheld by social media algorithms. [17] By protecting these three kinds of public interests, the right to know algorithms would, in certain situations, take precedence over social media companies' trade secret rights concerning their algorithms.[18] Indeed, the right to know and various regulatory

---

democratic check on the government); Thomas I. Emerson, *Legal Foundations of the Right to Know*, 1976 WASH. U. L.Q. 1, 4-5 (1976).

[14] *See infra* Part I.A; Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 60 (2019) ("In the context of artificial intelligence, we see a world where, at times, intellectual property principles prevent civil rights from adequately addressing the challenges of technology, thus stagnating a new generation of civil rights altogether."); Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085, 1138 (2018) ("Often, when [algorithmic] models are employed to change a way of making decisions, too much focus is placed on the technology itself instead of the policy changes that either led to the adoption of the technology or were wrought by its adoption.").

[15] *See* Brendan Zdunek, *Coca-Cola's Clandestine Operation: The Story and the Rationale Behind the World's Greatest Trade Secret* (Dec. 15, 2022), https://blogs.luc.edu/ipbytes/2022/12/15/coca-colas-clandestine-operation-the-story-and-the-rationale-behind-the-worlds-greatest- trade-secret/ [https://perma.cc/6MDC-NTMD].

[16] *See* PASQUALE, THE BLACK BOX SOCIETY, *supra* note 5, at 13 ("Google rose to the top of the tech pack while zealously guarding its 'secret sauce'—the complex algorithms it used to rank its sites."); Kristine Forderer, *Trade Secrets: A Valuable Tool in Your IP Protection Strategy* ( Jan. 22, 2021), https://www.cooleygo.com/trade-secrets-a-valuable-tool-in-your-ip-protection-strategy/#page=1 [https://perma.cc/RWP3-QNP6].

[17] *See infra* Part III.B.

[18] *See infra* Part II.A.

laws have demonstrated that public interests can prevail over private interests under specific circumstances.[19]

Second, the right to know would redefine the responsibilities of social media companies through offering a dynamic approach to algorithmic *responsibility*. It seeks to ensure that social media companies' trade secret rights in their algorithms are infused with responsibilities to facilitate algorithmic transparency for both their users and society at large in the public interest. It thus embraces the contention that innate to any legal right is a corresponding responsibility.[20] Therefore, the right to know imposes on social media companies a legal responsibility to make proportionate disclosure of their algorithms. Without such a responsibility, there is no doubt these companies would continue to maintain their algorithms in a black-box manner given their commercial value as trade secrets and their associated competitive advantages.

Through neutralizing algorithmic secrecy, the right to know social media algorithms would bring about policy changes and legal reforms. The most important policy change it could usher in is to better protect the interests of audiences for online information in the age of social media powered by artificial intelligence. Conventionally, legal regulation of social media in the United States has focused on ensuring that speakers can freely express their views on social media platforms. [21] However, this article argues that it is time for the American legal system to enhance the protection of audiences' interests through the right to know social media algorithms.

Social media platforms generate and disseminate an overwhelming amount of content through their algorithms, over-amplifying or suppressing information and making it challenging for audiences to find reliable, relevant information. Therefore, he recognition and protection of the right to know social media algorithms matters tremendously. The conventional wisdom that knowledge is power and ignorance weakness[22] applies perfectly to the new algorithmic age. By prioritizing audiences' interests, we can ensure that they are exposed to accurate, valuable, and diverse content, rather than being inundated with misleading or irrelevant information controlled by algorithms. In a democratic society, the free flow of reliable information and diverse perspectives is vital for

---

[19] Myrl L. Duncan, *Reconceiving the Bundle of Sticks: Land as a Community-Based Resource*, 32 ENVTL. L. 773, 794 (2002) (pointing out the doctrine of usufruct "created correlative public and private rights. Private rights were held subject to the overriding community interest.").

[20] *See* HAOCHEN SUN, TECHNOLOGY AND THE PUBLIC INTEREST 157-58 (2022).

[21] *See* Leslie Kendrick, *Are Speech Rights for Speakers?*, 103 VA. L. REV. 1767, 1808 (2017) ("First Amendment case law often focuses on speakers to the detriment of listeners."); Erin L. Miller, *Amplified Speech*, 43 CARDOZO L. REV. 1, 5 (2021) ("The core speakers' interests are autonomy and political participation. It is these core interests—which ultimately account for the protection of a very broad range of speech—that matter for the purposes of constitutional interpretation.").

[22] *See* Letter from Thomas Jefferson to Joseph C. Cabell (Dec. 25, 1820) ("[T]here can be no stronger proof that knowledge is power, and that ignorance is weakness."). The phrase "knowledge is power" is often attributed to Francis Bacon, from his *Meditationes Sacrae* (1597). *See* JOHN BARTLETT, FAMILIAR QUOTATIONS 168 (10th ed., 1919).

civic engagement with informed decision-making. By valuing audiences' interests, we can work towards creating a digital landscape that upholds these democratic values and allows for a more inclusive and informed public discourse. Hence, prioritizing audiences' interests through the right to know social media algorithms is essential for fostering a transparent, diverse, and accurate information ecosystem that benefits both individuals and society at large.

This article further shows how the right to know can facilitate legal reforms aimed at making social media companies more legally and socially responsible. In the present U.S. regulatory framework, these companies have minimal responsibilities.[23] For example, Section 230 of the Communications Decency Act shields social media companies from legal liabilities incurred by the content posted on their platforms by users.[24] To date, Congress has not enacted any specific law regulating social media algorithms.[25] Nevertheless, cases like *Gonzalez v. Google LLC*[26] and the emergence of legislative proposals addressing algorithmic accountability are prompting a comprehensive reevaluation of social media companies' responsibilities.

Implementing the right to know social media algorithms is a crucial aspect of the relevant legal reforms. This article demonstrates that this novel legal right would foster algorithmic transparency, intelligibility, and accountability as guiding principles for these reforms, prompting legislative, administrative, and judicial examinations of the appropriate extent to which social media companies should disclose confidential information regarding their algorithms.

Another advantage of this legal right is its foundation in the United States' long-established right to know. Rather than relying on the right to explanation found in foreign jurisdictions such as the European Union (E.U.), it is conceptually sound and practically viable to initiate legal reforms through a right to know social media algorithms in the United States. Further, while the right to explanation protects only personal data, the right to know social media algorithms offers broader legal protection covering personal data and other kinds of interests in the regulation of fake news and copyrighted materials by content moderation algorithms. [27]

---

[23] *See infra* Part III.A. *See also* SUn, *supra* note 20, at 108-09 (2022) ("Swayed by shareholder value theory, the US Congress has enacted major statutes that minimize the legal liability of technology companies ").

[24] *See* SUn, *supra* note 20 at 109 ("Congress enacted the Communication Decency Act (CDA) in 1996 as a legal tool to provide internet service providers with immunity from platform users' illegal activities. "); Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 657 (2014); Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 402-06 (2017).

[25] *See infra* Part IV.

[26] Robert Barnes et al., *Supreme Court Considers If Google is Liable for Recommending ISIS Videos*, WASH. POST (Feb. 21, 2023), https://www.washingtonpost.com/technology/2023/02/21/gonzalez-v-google-section-230-supreme-court/ [https://perma.cc/HN9W-K4U8] ("The Supreme Court on Tuesday heard oral arguments in Gonzalez v. Google, a lawsuit that could shift the foundations of internet law. It argues tech companies should be legally liable for harmful content their algorithms promote.").

[27] *See infra* Part IV.A. 3.

The remainder of the article proceeds as follows. Part I shows ways in which IP law protects social media algorithms as trade secrets, entitling their rights owners to maintain exclusive control over their secrecy. Drawing on the right to know protected by freedom of information laws, Part II provides justifications for recognition of the right to know algorithms. It demonstrates that this new legal right would better protect the public interest in democrat- ic participation, public safety and social equality. Part III explores why the right should prevail over trade secret rights in social media algorithms. Rely- ing upon the new legal right's information disclosure power, Part IV puts forward a multi-stakeholder approach to regulating algorithmic secrecy through legislative actions, administrative oversight, and judicial protection. It also considers the advantages of this approach over several other proposals for addressing algorithmic secrecy and clarifies how it would not violate the First and Fifth Amendments to the U.S. Constitution.

## I. Protecting Social Media Algorithms as Trade Secrets

### A. *Meeting the Legal Requirements of Trade Secret Protection*

Trade secret law protects commercially valuable information that is kept confidential. Trade secrets include technical information, such as manufacturing methods, chemical processes, formulas, and related equipment.[28] Typical examples are the Coca-Cola formula and computer program source codes. Trade secrets may also include non-technical business information, such as customer lists, marketing data and strategies, and geological data and genetic information collected from business activities.[29]

The algorithms employed by social media platforms trigger computational processes involved in the gatekeeping of content.[30] They are black boxes that are developed in a confidential manner[31] and legally protected as trade secrets. Under the Uniform Trade Secrets Act (USTA) [32] and Defend Trade Secrets

---

[28] *See* Elizabeth A. Rowe & Sharon K. Sandeen, Trade Secret Law: Cases and Materials 51 (2020).

[29] *See* Deepa Varadarajan, *Trade Secret Fair Use*, 83 Fordham L. Rev. 1401, 1407 (2014).

[30] Zeynep Tufekci, *Algorithmic Harms beyond Facebook and Google: Emergent Challenges of Computational Agency*, 13 Colo. Tech. L.J. 203, 206 (2015).

[31] *See e.g.* Mark van Rijmenam, *Algorithms are Black Boxes, What is Why We Need Explainable AI*, Medium (Sept. 4, 2019), https://markvanrijmenam.medium.com/algorithms-are-black-boxes-that-is-why-we-need-explainable-ai-72e8f9ea5438 [https://perma.cc/D3FB-F83T]; Kaveh Waddell, *Tech Companies Too Secretive About Algorithms That Curate Feeds, Study Says*, Consumer Rep. (Feb. 24, 2021), https://www.consumerreports.org/consumer-protection/tech-companies-too-secretive-about-algorithms-that-curate-feeds-a8134259964/ [https://perma.cc/Q5WU-UUHU]; Frederick Mostert, *Social Media Platforms Must Abandon Algorithmic Secrecy*, Fin. Times ( June 17, 2021), https://www.ft.com/content/39d69f80-5266-4e22-965f-efbc19d2e776 [https://perma.cc/9DND-H5LR ].

[32] *See* Sharon K. Sandeen & Christopher B. Seaman, *Toward a Federal Jurisprudence of Trade Secret Law*, 32 Berkeley Tech. L.J. 829, 833 (2017).

Act (DTSA),[33] trade secrets are defined as information that is non-public, that has been subject to reasonable protection measures, and that derives independent economic value from remaining secret.[34] Social media companies' algorithms fulfil these conditions for trade secret protection, as explained below.

First, social media algorithms have "independent economic value." In practice, some courts have been willing to presume that such value exists based on the mere existence of a lawsuit, but the value requirement is actually more complex.[35] In legislative history, "economic value" has been considered synonymous with "commercial value," which may consist of "actual value" established through direct or circumstantial evidence or "potential value" in cases where actual value is difficult to prove.[36] However, what is most important is that this value is "independent," that what is being protected has "value that is separate and apart from its value to the trade secret owner; that is, it must also have value to *others*."[37]

The actual economic value of algorithms is evident. Social media platforms are some of the most lucrative attention economy businesses, selling user engagement as a product to advertisers.[38] Algorithms that can accurately predict the content that users want to see capture users' attention for longer, and thus offer competitive advantages to the platforms that own them.[39] The comparative success of social media algorithms is frequently based on their ability to generate a high percentage of views or clicks. For instance, YouTube's algorithms were lauded as a success in 2018, being credited as the source of 70% of total user watch time.[40] TikTok's algorithms generate perhaps as much as 95% of user watch time, and its parent company ByteDance has begun selling parts of its algorithms to other companies.[41] These figures certainly suggest the "independent economic value" of platforms' algorithms.

---

[33] *Id.* at 833.

[34] *See* John Cannan, *A (Mostly) Legislative History of the Defend Trade Secrets Act of 2016*, 109 LAW LIBR. J. 363, 364 (2017).

[35] THOMAS G. SPRANKLING, UNDERSTANDING TRADE SECRET LAW 32 (2020).

[36] *Id.* at 32-34 (For actual value "[o]ften the most convincing direct evidence is that the defendant has used the plaintiff 's information to successfully provide the same service or product to customers" and circumstantial evidence can include '(1) the time and money that the plaintiff invested to develop the secret; (2) the plaintiff 's use of the information; (3) the willingness of others to pay for the information; and (4) the defendant's efforts to obtain the information'. Although "the precise meaning of 'potential' value is far from clear", courts have considered defendant conduct as evidence that information without any obvious "actual value" has, at least, "potential value.").

[37] *Id.* at 32.

[38] Vikram R. Bhargava & Manuel Velasquez, *Ethics of the Attention Economy: The Problem of Social Media Addiction*, 31 BUS. ETHICS Q. 321, 321 (2021).

[39] Isamu Nishijima, *TikTok's Secret Moneymaker is Actually its Algorithms*, MEDIUM (Aug. 19, 2021), https://medium.com/headlineasia/tiktoks-biggest-money-maker-is-actually-an-algorithm-879c5518db53 [https://perma.cc/E6XQ-QRT3].

[40] NOAH GIANSIRACUSA, HOW ALGORITHMS CREATE AND PREVENT FAKE NEWS 70 (2021).

[41] *See* Nishijima, *supra* note 39; Hayden Field, *ByteDance is Selling TikTok's "For You" Algorithm to Other Companies*, EMERGING TECH BREW (July 7, 2021), https://www.emergingtech-

Second, social media algorithms are "not generally known" or "readily ascertainable by proper means." *Relative*, not absolute, secrecy is required for trade secret protection.[42] Even if two or more companies in the same industry have knowledge of an algorithm, it may still be eligible for protection if it does not constitute general industry knowledge.[43] Although proving the absence of knowledge can be difficult, courts have been willing to accept circumstantial evidence, including (1) statements from experts concerning the novelty of the information concerned, (2) the willingness of others to pay for the information, (3) the defendant's misappropriation of the information, and (4) the issuance of patents based on the information.[44] Where information is not generally known, protection may still be denied if others could potentially acquire or reproduce it with relative ease.[45] However, such acquisition or reproduction must arise from (1) independent invention, (2) reverse engineering, (3) discovery under a license granted by the plaintiff, (4) observation during public use or display, or (5) published literature.[46] Information is therefore protected if it is readily ascertainable only through such improper means as theft, bribery, or misrepresentation.[47]

Social media algorithms meet this requirement because they are not generally known to the tech sector or the public at large. Public discourse on social media algorithms commonly concerns the air of mystery surrounding them.[48] The public is aware that algorithms are a feature of platform services, but unaware of exactly how they work.[49] Social media platforms invest significant amounts in ensuring a constantly increasing level of accuracy in content recommendation and level of technical sophistication in their processes.[50] They all employ algorithms for similar purposes but have independent strategies for maximizing value. If platforms wish to imitate the algorithms of their competitors, they can only look at the outcomes generated and attempt to replicate them. For instance, in response to the "extended backlash against social media starting in 2016," YouTube changed its algorithmic recommendation policy to prioritize "valued watchtime," and Facebook shifted to a focus on "time well

---

brew.com/stories/2021/07/07/bytedance-selling-tiktoks-algorithm-companies [https://perma.cc/6PVF-JAVJ].

[42] *See* SPRANKLING, *supra* note 35, at 34.

[43] *Id.* at 35.

[44] *Id.* at 35-36.

[45] *Id.* at 38-41.

[46] *Id.* at 41.

[47] *Id.*

[48] *See e.g.* Waddell, *supra* note 31; Mostert, *supra* note 31; Laura Dodsworth, *What's the Truth About Facebook and Twitter's Algorithm Riddle?*, SPECTATOR (May 17, 2022), https://www.spectator.co.uk/article/what-s-the-truth-about-facebook-and-twitter-s-algorithm-riddle-[https://perma.cc/X6EH-LT8E].

[49] Dodsworth, *supra* note 48.

[50] Will Oresmus *et al*., *How Facebook Shapes Your Feed*, WASH. POST (Oct. 26, 2021), https://www.washingtonpost.com/technology/interactive/2021/how-facebook-algorithm-works/ [https://perma.cc/6L7T-WVW7].

spent."[51] However, because of concerns over TikTok's ability to hold users' attention, both YouTube and Facebook have since altered their algorithms to promote their own short video services, which employ the same format as TikTok's, in an attempt to replicate their impact.[52] Moreover, the fact that TikTok has customers willing to pay for access to its algorithmic recommendation expertise suggests that that expertise is not generally known within the industry.[53]

Finally, social media platforms take reasonable precautions to maintain the secrecy of their algorithms. Such precautions can be broadly categorized as procedures designed to ensure security or to ensure confidentiality.[54] They must be directed toward the prevention of misappropriation by both *outsiders* and *insiders*, including employees, suppliers, customers, and licensees.[55] In *Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.*,[56] the court held that "reasonable efforts" to maintain secrecy should be assessed on the basis of "a balancing of costs and benefits that will vary from case to case."[57] Examples include advising employees of the existence of the trade secret concerned, limiting awareness to those who need to know, and limiting physical access, although the variability of the reasonable precaution standard means that these measures will not apply in every case.[58] Reasonable precautions are increasingly difficult to take in the digital age, as large amounts of data are now stored in the cloud, and thus under the control of third parties.[59] However, efforts to maintain secrecy can include (1) company policies concerning the types of information that may be stored in the cloud; (2) confidentiality agreements with third-party storage space providers; (3) physical security measures at server sites; and (4) security protocols such as data encryption, layers of authentication, and rules against the downloading of information onto personal devices.[60]

The existence of security measures in the context of social media algorithms is evidenced by the difficulties researchers have encountered in investigating the effects of recommendation technology. For instance, after researchers found that 70% of videos flagged as containing misinformation in their study of YouTube had been recommended by the platform's algorithms, commentators expressed concern that further study of the finding was impossible "because the algorithm is a closely-guarded secret at Google."[61] Similarly, Facebook was accused of preventing New York University researchers from

---

[51] Mark Bergen, *Inside YouTube's Secret Algorithm Wars*, OBSERVER (Sept. 13, 2022), https://observer.com/2022/09/inside-youtubes-secret-algorithm-wars/ [https://perma.cc/GUZ8-ZDDG].

[52] *Id.*

[53] *See* Nishijima, *supra* note 39.

[54] DOUGLAS G. CHISUM ET AL., UNDERSTANDING INTELLECTUAL PROPERTY LAW 216 (2011).

[55] *See* SPRAUKLING, *supra* note 35, at 43.

[56] 925 F.2d 174 (7th Cir. 1991).

[57] *Id.* at 179; *See* SPRAUKLING, *supra* note 35, at 44.

[58] *See* SPRAUKLING, *supra* note 35, at 44.

[59] *Id.* at 46.

[60] *Id.*

[61] Ben Gilbert, *YouTube's Secret Algorithm Continues to Push Misinformation on Users, From False Election Fraud Claims to Conspiracy Theories, According to New Studies*, BUS. INSIDER (July 7,

looking into social media-generated electoral distrust after claiming that they had been gathering information improperly.[62]

Evidence of social media platforms' protection of algorithm-adjacent information pertaining to platform moderation and recommendation processes can also be seen in Facebook's response to recent whistleblowing actions. After former employee Frances Haugen went public with concerns about Facebook's practices, new policies were implemented to limit internal access to research addressing sensitive topics, including radicalization and mental health. In addition, "researchers said they have been asked to submit work on sensitive topics for review by company lawyers, who have sometimes asked for examples of problems to be excised from internal posts."[63]

### B. *Applying Commercial Strategies for Trade Secret Protection*

Algorithms are set to become a critical component of every business because almost all of the business insights and decisions of tomorrow will be data-driven. The application of algorithms to leverage data that can be used to optimize processes or create revenue streams is widespread across many industries. From automotive anti-lock braking to Amazon's recommendation engine, from dynamic pricing for airlines to predicting the success of upcoming Hollywood blockbusters, from credit card fraud detection to the 2% of posts that Facebook shows a typical user and Uber's matching of drivers with passengers, algorithms permeate every aspect of modern life.[64]

Practically, protecting social media algorithms as trade secrets accords with technology companies' corporate strategies. First, trade secrets have useful advantages over other forms of intellectual property (IP) protection. Unlike copyrights or patents, trade secrets are protected for as long as they are not disclosed, and therefore potentially never expire.[65] Taking the trade secret protection route can be risky and unpredictable, however, as events beyond the owner's control may lead to disclosure, and hence to destruction of the trade secret.[66] That said, similar uncertainty exists in relation to patents owing to the possibility of rights being terminated before the expiration of the patent term.

---

2021), https://www.businessinsider.com/youtube-algorithm-continues-to-push-misinformation-study-finds-2021-7 [https://perma.cc/9TY4-6WLK].

[62] Paul Barrett, Justin Hendrix & Grant Sims, *How Tech Platforms Fuel U.S. Political Polarization and What Government Can Do About it,* BROOKIUgS (Sept. 27, 2021), https://www.brookings.edu/blog/techtank/2021/09/27/how-tech-platforms-fuel-u-s-political-polarization-and-what-government-can-do-about-it/ [https://perma.cc/8KSY-AZU6].

[63] Keach Hagey *et al.*, *Facebook's Pushback: Stem the Leaks, Spin the Politics, Don't Say Sorry*, WALL ST. J. (Dec. 29, 2021), https://www.wsj.com/articles/facebook-whistleblower-pushback-political-spin-zuckerberg-11640786831 [https://perma.cc/5946-SJ7A].

[64] Salim Ismail, *Why Algorithms Are 7e Future Of Business Success*, GROWTH IUSTITUTE, https://blog.growthinstitute.com/exo/algorithms [https://perma.cc/FD2C-LQEV].

[65] *See* Camilla A. Hrdy & Mark A. Lemley, *Abandoning Trade Secrets*, 73 STAu. L. REV 1, 12 (2021).

[66] Andrew Beckerman-Rodau, *7e Choice between Patent Protection and Trade Secret Protection: A Legal and Business Decision*, 84 J. PAT. & TRADEMARK OFF. SOC'Y 371, 384 (2002).

Also, in the case of simultaneous invention, creators can be prevented from using their own technology if they lose a U.S. Patent and Trademark Office (PTO) interference action.[67] The fact that perpetual protection is the best- case scenario leads some to prefer the risk of trade secret disclosure to the risk of patent invalidation.[68] Other advantages of trade secrets include (1) the absence of arduous application procedures or requirements,[69] (2) the lack of public disclosure requirements,[70] and (3) their ability to tie useful employees to the company for longer.[71]

Assessing social media algorithms by some of the factors that businesses typically consider when deciding between different forms of protection demonstrates why many platforms opt for trade secrets. Businesses generally compare the life cycle of their inventions against both the 20-year term of patent protection and the typical and costly 24-month period required to obtain a patent.[72] Social media algorithms require frequent updates,[73] meaning that the effort to secure 20 years of protection through an expensive 24-month process is unlikely to be worthwhile for platforms. Businesses also typically consider the likelihood of proprietary information being exposed through legal means.[74] As demonstrated below, the risk of reverse engineering is low in the case of social media algorithms.[75] Most importantly, businesses typically consider whether the information or technology concerned is actually eligible or suitable for other forms of IP protection,[76] a factor that further encourages algorithm owners to protect their algorithms as trade secrets.

---

[67] *Id.* at 384-85.

[68] Andrew A. Schwartz, *The Corporate Preference for Trade Secret*, 74 OHIO ST. L.J. 623, 632 (2013).

[69] *Id.* at 629 ("All that is required is that the holder of the trade secret takes reasonable precautions to prevent its disclosure.").

[70] David S. Levine & Ted Sichelman, *Why Do Startups Use Trade Secrets*, 94 NOTRE DAME L. REV. 751, 757 (2018) ("Although startups can maintain a lead-time advantage simply because of the inherent failure of competitors to innovate, a primary reason for choosing trade secrecy is to extend a lead-time advantage by preventing the disclosure of specific information that provides the advantage."); Katarina Foss-Solbrekk, *Three Routes to Protecting AI Systems and Their Algorithms Under IP Law: The Good, the Bad and the Ugly*, 16 J. INTELL. PROP. L. & PRACTICE 247, 256-57 (2021).

[71] *See* Levine & Sichelman, *supra* note 70, at 767 ("Startups are often faced with key employees wishing to depart for a competitor or to form a new company. A noncompetition agreement, which prevents employees from working at a competitor for a specified period of time after termination or resignation, is the primary mechanism to stem this leakage of 'human capital.' Where enforced, they can be very effective at preventing employees from working for a competitor.").

[72] Meghan J. Ryan, *Secret Algorithms, IP Rights, and the Public Interest*, 21 NEV. L.J. 61, 71-72 (2020).

[73] Hannah Trivette, *A Guide To Social Media Algorithms And SEO*, FORBES (Oct. 14, 2022), https://www.forbes.com/sites/forbesagencycouncil/2022/10/14/a-guide-to-social-media-algorithms-and-seo/?sh=593e1fcf52a0 [https://perma.cc/4VTT-8V5W].

[74] *See* Ryan, *supra* note 72.

[75] *See id.*

[76] *See id.*

Second, other forms of IP protection are less suited to the technical nature of algorithms. Despite the Copyright Act explicitly providing copyright protection to computer programs, there is considerable uncertainty over the scope of the protection afforded them, as they do not "fall squarely within traditional copyright subject matter like literary manuscripts," instead being "mostly functional in nature even though [the algorithm] is expressed in text through source and object code."[77] Although an algorithm's source and object code are unquestionably protected against literal infringement, such protection does not prevent other computer programmers from rewriting the source code to achieve the same function using a different expression.[78]

Patent law is a similarly uncertain source of algorithm protection for social media platforms. Even before considering the complex question of whether algorithms are novel, useful, and non-obvious, "whether computer programs . . . are at all patentable remains a contentious topic."[79] In the U.S., in the just two years following *Alice Corp. v. CLS Bank International*,[80] wherein the Supreme Court held that the application of an abstract idea on a computer-implemented service was not patentable unless it involved an inventive concept,[81] it was estimated that the PTO had rejected approximately 60,000 patent applications and that prosecutors had abandoned about 8,400 applications.[82] Moreover, U.S. courts have strengthened the non-obviousness standard by shifting focus from success in the piecing together of prior art to "common sense, market demand, or design trends."[83] These developments have "pushed software developers deeper into the world of trade secrets"[84] and further away from patent protection and the public disclosure it ensures.

## II. Recognizing the Right to Know Social Media Algorithms

In this part, I argue that it is necessary to recognize the right to know algorithms as a new legal right protecting the public interest in today's algorithmic society. I first consider how international human rights law and domestic freedom of information laws have employed the right to know in protecting democratic governance, public safety, and social equality. The critical importance of these three kinds of public interest in the algorithmic age justifies the ushering in of a right to know social media algorithms.

---

77 *Id.* at 73-74.
78 *Id.* at 74.
79 *See* Foss-Solbrekk, *supra* note 70, at 253.
80 573 U.S. 208 (2014).
81 *Id.*
82 *See* Ryan, *supra* note 72, at 83.
83 *Id*. at 84-85; Nautilus, Inc. v. Biosig Instruments, Inc., 134 S. Ct. 2120, 2124 (2014).
84 *See* Ryan, *supra* note 72, at 87.

### A. *The Right to Know and the Public Interest*

The right to know, also referred to as the "right to information"[85] or "freedom of information,"[86] was coined by a journalist in 1945.[87] It is intended to empower people to obtain sufficient information about decisions that affect them, thereby holding decision-makers, such as governments, accountable.[88] Originally, the right to know was mostly justified as a legal right safeguarding the public interest in participation in democratic institutions.[89] Recent decades, however, have seen the expansion of this legal right to protect other public interests. In particular, the right protects people's freedom to know about environmental hazards and to give informed consent.[90]

Hence, I suggest in this section a broad-based approach to justifying legal protection of the right to know, demonstrating that it is a legal right protecting public interests concerned not only with democratic governance but also with public safety and social equality. Therefore, the right to know entitles citizens to have access to the information held by government agencies as well as the information held by certain private entities that may affect the three kinds of public interest identified in this section below.

#### 1. Democratic Participation

Akin to freedom of expression, the right to know is politically central to the maintenance of dynamic democratic participation in modern societies. Key to any effective democracy is the imposition of checks on those who hold political power. Any governmental agency or official has a tendency to abuse such power. As James Madison observed, "If Men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which

---

[85] *See* UNESCO, *Right to Information*, https://www.unesco.org/en/right-information [https://perma.cc/K9XY-GQ57] ("UNESCO advocates for access to information as a fundamental freedom and a key pillar in building inclusive knowledge societies.").

[86] *See* RICHARD A. CHAPMAN, FREEDOM OF INFORMATION: LOCAL GOVERNMENT AND ACCOUNTABILITY 125 (2001).

[87] Associated Press journalist Kent Cooper stated that "Citizens are entitled to have access to news, fully and accurately presented. There cannot be political freedom in one country, or in the world, without respect for 'the right to know.'" *See* MICHAEL SCHUDSON, THE RISE OF THE RIGHT TO KNOW: POLITICS AND THE CULTURE OF TRANSPARENCY, 1@AB–1@CB 7 (2015).

[88] According to UNESCO, the right to know is defined as a right for people to "participate in an informed way in decisions that affect them, while also holding governments and others accountable." UNESCO, FREEDOM OF INFORMATION: THE RIGHT TO KNOW 16 (2011).

[89] *See*, *e.g.*, Barry Sullivan, *FOIA and the First Amendment: Representative Democracy and the People's Elusive Right to Know*, 72 MD. L. REV. 1, 9 (2012) (demonstrating that the right to know promotes government accountability and citizen participation); Thomas I. Emerson, *Legal Foundations of the Right to Know*, 1976 WASH. U. L.Q. 1, 16 (1976) ("One would seem to be on solid ground, therefore, in asserting a constitutional right in the public to obtain information from government sources necessary or proper for the citizen to perform his function as ultimate sovereign.").

[90] *See generally* THE PEOPLE'S RIGHT TO KNOW MEDIA, DEMOCRACY, AND THE INFORMATION HIGHWAY (Frederick Williams & John V. Pavlik eds., 1994); Rajeev Kumar Singh, *Right to Information: The Basic Need of Democracy*, 1 J. EDUC. & SOC. POL'Y 86 (2014).

is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place, oblige it to control itself."[91] Institutionally, democratic mechanisms, such as elections and the separation of powers, are designed to guard against the abuse of political powers by delimiting those powers.

Procedurally, the right to know empowers citizens to require the disclosure of political governance information to the greatest extent possible, thereby preventing government agencies and officials from concealing information and creating an environment that breeds abuses of power. Madison also asserted that a "popular government without popular information or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors must arm themselves with the Power which knowledge gives."[92] The means of accessing the information held by the government, as Madison emphasized, entails statutory or administrative procedures that citizens can follow to demand the disclosure of that information. The right to know ensures the availability of such procedures by requiring the government to make them available to citizens when their need for access to information arises.

Substantively, the right to know also functions to nurture citizens' capacities in limiting governmental power.[93] As watchdogs of the government, citizens must obtain sufficient knowledge of its decisions before they can play their oversight role.[94] Access to adequate information is crucial for making informed, self-governing decisions. The ability to seek and obtain pertinent information is an essential prerequisite for individuals to make such decisions. Knowledge equates to power, while ignorance results in powerlessness.[95] The extent of one's knowledge dictates one's capability to make well-founded decisions, which in turn influences our capacity to address and mitigate risks. Consequently, an informed citizenry serves as a safeguard against risks posed by government abuse and corruption.[96] As Justice Brennan aptly pointed out, disclosing information about government activities is vital to "ensure that the individual citizen can effectively participate in and contribute to our republican system of

---

[91] James Madison, *Federalist Papers No. 51* (1788), https://billofrightsinstitute.org/primary-sources/federalist-no-51 [https://perma.cc/5ZW2-S8XZ].

[92] James Madison, *Epilogue: Securing the Republic* (1822), https://press-pubs.uchicago.edu/founders/documents/v1ch18s35.html [https://perma.cc/9HNG-34AE].

[93] Branzburg v. Hayes, 408 U.S. 665, 721 (1972) (Douglas, J., dissenting) ("The right to know is crucial to the governing powers of the people.").

[94] New York Times Co. v. United States, 403 U.S. 713, 717 (1971) (Black, J., concurring) ("The press was to serve the governed, not the governors. ..... The press was protected so that it could bare the secrets of government and inform the people.").

[95] *See generally* LAuI WATSOu, THE RIGHT TO KuOW: EPISTEMIC RIGHTS AuD WHY WE NEED THEM (2021).

[96] The Supreme Court stated that "informed public opinion is the most potent of all restraints upon misgovernment." Grosjean v. American Press Co., 297 U.S. 233, 250 (1936).

self-government."[97] Failure to protect the right to know through such information disclosure runs counter to the ideal of a well-informed citizenry.[98]

Given the importance of the right to know in promoting democratic governance, international human rights treaties first recognized this legal right as part of freedom of expression. Article 19 of the Universal Declaration of Human Rights[99] states that the liberty to seek, receive, and impart information and ideas is an integral part of freedom of opinion and expression. Article 19 of the International Covenant on Civil and Political Rights[100] protects the right to know in the same way.

Domestic laws also recognize and protect the right to know. In the United States, the Freedom of Information Act (FOIA) grants individuals the legal right to access government information. Enacted in 1966, the FOIA was a response to concerns about government secrecy and the denial of information requests from the press by executive agencies. Its purpose was to ensure that government agencies respected the public's right to know.[101] In addition to mandating the publication of certain agency materials, the FOIA also requires federal agencies to release other requested information. [102] As aptly stated by the U.S. Supreme Court, "FOIA is . . . a means for citizens to know what the Government is up to."[103] Protecting the right to know through statutory measures is therefore essential for the proper functioning of a democracy.

Under the FOIA, the right to know is a public right because its information disclosure obligations are grounded in the public interest in democratic participation. The scope of information disclosure required by the FOIA is extraordinarily broad, although it recognizes such statutory exemptions as national security and personal privacy. According to the FOIA guide, "virtually every record possessed by a government agency" is releasable "unless it is specifically exempted from disclosure or specifically excluded from the Act's cov-

---

[97] Whitney v. California, 274 U.S. 357, 362 (1927).

[98] WATSOU, *supra* note 95, at 82 (arguing that injustifiably limiting the free flow of information will cause "diminished decision-making"); Michael J. Perry, *Freedom of Expression: An Essay on Theory and Doctrine*, 78 NW. U. L. REV. 1137, 1195 (1983) (arguing that "government denial of access to protected information . . . subverts the ideal of a knowledgeable citizenry, a well-informed electorate, without which democracy is a sham.").

[99] G.A. Res. 217 (III) A, Universal Declaration of Human Rights, (Dec. 10, 1948). Article 19 states that "[e]veryone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

[100] 999 U.N.T.S. 171; S. Exec. Doc. E, 95-2 (1978); S. Treaty Doc. 95-20; 6 I.L.M. 368 (1967). Article 19 of the Covenant states that "[e]veryone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."

[101] BENJAMIN M. BARCZEWSKI & MEGHAN M. STUESSY, CONG. RSCH. SERV., IF11EFG, CONGRESS AND THE FREEDOM OF INFORMATION ACT (FOIA) 1 (2023), https://crsreports.congress.gov/product/pdf/IF/IF12301 [https://perma.cc/WKY7-873X].

[102] *Learn about FOIA*, FREEDOM OF INFORMATION ACT, https://www.foia.gov/about.html [https://perma.cc/QU3H-EL7S].

[103] Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157, 160 (2004).

erage."[104] Any individual, organization, or media outlet has a statutory right to petition a government agency for a FOIA-based request because "[t]he disclosure does not depend on the identity of the requester. As a general rule, if the information is subject to disclosure, it belongs to all."[105]

2. Public Safety

Socially and economically, the right to know plays a pivotal role in safeguarding public interests in societal safety issues ranging from environmental protection and health care to market order.[106] It ensures that members of the public can acquire sufficient information pertinent to these public interests to make well-informed decisions.

Environmental protection is one of the most salient public safety interests protected by the right to know. By requiring the government and/or private stakeholders to disclose information about environmental hazards, this legal right empowers individuals and society as a whole to proactively address such risks. The impetus for greater transparency in this regard stemmed from a series of tragic incidents that resulted in numerous deaths and widespread toxin contamination. One such example is the Bhopal disaster in India, which occurred in December 1984 when a cloud of methyl isocyanate escaped from an insecticide plant, claiming the lives of 15,000 people and causing injuries to countless others. Prior to this catastrophe, the plant's abysmal safety record and the absence of evacuation or emergency plans had already been identified. However, the lack of awareness and knowledge within the community about the dangers posed by the plant allowed this entirely preventable disaster to unfold.[107]

In the aftermath of the Bhopal disaster, U.S. Congress passed the Emergency Planning and Right to Know Act of 1986. This act marked the first legislative effort to inform the public about the pollution activities of corporations. Its main provision mandates that industrial facilities throughout the United States must disclose information regarding their annual release of toxic chemicals. These data are then included in the Environmental Protection Agency's Toxics Release Inventory, which is accessible to the public. While considered a positive step forward, the Act has limitations. It only requires companies to disclose the quantity of individual pollutants they release, without any obligation to provide information about toxicity, spread, or potential overlaps. [108]

---

[104] OFFICE OF IuFO. & PRIVACY, U.S. DEP'T OF JUSTICE, FREEDOM OF IuFORMATIOu ACT GUIDE & PRIVACY ACT OVERVIEw 5 (2000).

[105] *Nat'l Archives C Records Admin.*, 541 U.S. at 172.

[106] UNESCO, *supra* note 85 ("Access to information . . . is an enabler for sustainable development in areas such as health, environment, addressing poverty and fighting corruption."); UNESCO, *supra* note 88, at 14 ("Freedom of information is often associated with well-functioning markets and improvements in investment climates.").

[107] *See* Shannon M. Roesler, *7e Nature of the Environmental Right to Know*, 39 ECOLOGY L.Q. 989, 1017 (2012).

[108] *Id*. at 1017-18.

The public also has a right to health information, access to which is considered essential to an effective public health protection system,[109] as it allows individuals to promote their own health by taking preventive measures and receiving proper medical treatment.[110] In other words, access to health information enables individuals to make well-informed decisions about their personal health. The robust circulation of health information plays a vital role in public healthcare systems. In normal circumstances, it helps medical professionals to devise strategies for coping with acute and chronic diseases. In extraordinary circumstances, such as epidemics, pandemics, and other public health crises, health information becomes a crucial component of crisis response measures, ranging from virus outbreak investigations to the development of treatments and vaccines.[111]

3. Social Equality

All human beings ought to enjoy dignity and freedom equally. Such social equality is enshrined as a core public interest in both international human rights treaties and national constitutions.[112] However, discrimination persists in the United States and many other countries. Against this backdrop, institutions should endeavor to minimize the impact of status discrimination and the

---

[109] Paul Hunt, *Report of the Special Rapporteur on the Right of Everyone to the Enjoyment of the Highest Attainable Standard of Physical and Mental Health*, U.N. DOC. A/HRC/7/11 (Mar. 21, 2008) https://ap.ohchr.org/documents/dpage_e.aspx?si=A%2FHRC%2F7%2F11 [https://perma.cc/CCC4-3JNQ] ("Access to health information is an essential feature of an effective health system, as well as the right to the highest attainable standard of health."); *Health Information and Public Health*, CTRS. FOR DISEASE COUTROL & PREVEUTIOU, (Sept. 24, 2018), https://www.cdc.gov/phlp/publications/topic/healthinformation.html [https://perma.cc/M86Z-6NEZ] ("Effective use of information is the foundation of modern public health practice.").

[110] ARTICLE i@, A HEALTHY KUOWlEDGE RIGHT TO IUFORMATIOU AUD THE RIGHT TO HEALTH (2012), https://www.article19.org/wp-content/uploads/2018/02/12-09-12-POLICY-right-to-health-WEB.pdf [https://perma.cc/W5PN-2DCM] ("Health information enables individuals and communities to promote their own health, participate effectively, claim quality services, monitor progressive realization, expose corruption, hold those responsible to account, and so on.").

[111] *Health Information and Public Health*, CTRS. FOR DISEASE COUTROL & PREVEUTIOU, (Sept. 24, 2018), https://www.cdc.gov/phlp/publications/topic/healthinformation.html [https://perma.cc/M86Z-6NEZ] ("Public health responses—such as outbreak investigations, prevention strategies for diseases such as cancer, and health system improvements to quality and performance—require timely, accurate health information. As a result, a range of public and private entities use health information to increase our knowledge about, and improve our response to, emerging public health issues, whether aggregated, de-identified, or attributed to individuals who need treatment.

Health information sources, such as electronic health records, health information exchanges, vital records, immunization information systems, syndromic surveillance systems, and other public health databases, can provide critically important data about specific population health needs and effective interventions to practitioners responsible for addressing public health and patient care.").

[112] For example, Article 1 of the Universal Declaration on Human Rights states that "[a]ll human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood."

unequal distribution of resources. Promoting social equality is widely regarded as the "first virtue of social institutions."[113]

Social equality is another public interest that the right to know protects. Certain groups of citizens, such as minorities and low-income people, are often excluded from governmental decision-making or have concealed from them information on the negative effects of government agency decisions.[114] A lack of access to information is thus very likely to cause discrimination on the basis of identity, race, income, gender, age, sexual orientation, language, disability, and/or religious belief.

The right to know seeks to address discriminatory government decisions that disproportionately affect specific groups of citizens. It necessitates that government agencies fulfill their responsibility to inform the individuals and communities impacted by these decisions of the potential risks or consequences involved.[115] Importantly, this duty exists regardless of whether the affected parties actively request the disclosure of such information. For instance, the U.S. government has issued executive orders that require federal agencies to guarantee equal participation from minority and low-income populations in their decision-making processes.[116]

Along with its procedural role in involving citizens in decision-making, the right to know also safeguards substantive interests in accessing government decision-making information. Governments worldwide invest significant resources in providing welfare services, particularly to disadvantaged citizens. However, they often pay less attention to disseminating information about these services to those who most need them. As a consequence, access to welfare services is frequently denied to those who require them the most. In this context, information serves as a gateway to services, and a lack of information equates to a lack of access and, consequently, discrimination.[117]

In Australia, the concepts of access and equity emerged as a policy response to address the challenges faced by individuals from non-English-speak-

---

[113] JOHN RAWLS, A THEORY OF JUSTICE 3 (rev. ed. 1999). Rawls also points out that "[a] theory however elegant and economical must be rejected or revised if it is untrue; likewise laws and institutions no matter how efficient and well-arranged must be reformed or abolished if they are unjust." *Id*.

[114] C.G. Weeramantry, *Access to Information: A New Human Right*, 4 ASIAN Y.B. INT'L L. 99, 119-20 (1994) ("Governments all over the world spend vast sums of money providing welfare services to citizens especially in the disadvantaged groups but perhaps devote insufficient attention to distributing information to those most in need of those services, with the result that those who need the services most may not have practical access to them. Information in this context means access to those services and lack of information means lack of access and *de facto* discrimination.").

[115] *Id*. at 119.

[116] *See* Exec. Order No. 12,898, 59 Fed. Reg. 7629 (Feb. 11, 1994), amended by Exec. Order No. 12,948, 60 Fed. Reg. 6381 (Feb. 1, 1995) (requiring federal agencies to ensure the equal participation of minority and low-income populations in decision making).

[117] See Michael Traber, *Communication as a Human Need and Human Right*, 39 RELIGION & SOC'Y 1, 9 (1992).

ing backgrounds in accessing government services.[118] The government recognized that these individuals encountered difficulties in obtaining information about the various programs available to them and their eligibility for different services.[119] Consequently, in 1989, it formally extended the Access and Equity Strategy to encompass all groups that might encounter barriers due to factors such as race, religion, language, or culture. This policy recognizes that access to information about government agencies, programs, services, and entitlements is both a right and a prerequisite for effectively utilizing the opportunities and resources provided by the government. Simultaneously, the government has a responsibility to inform citizens of their entitlements and actively promote its programs and services to them.[120]

### B. *Social Media Algorithms and the Public Interest*

Should we subject social media algorithms to the scrutiny of the right to know? Or to put it differently, should we recognize a new legal right to know algorithms? In this section, I first address this issue by demonstrating that people have interests concerned with democratic governance, public security, and social equality when it comes to social media algorithms. Given that the right to know is justified by these public interests, I argue that we should broaden the right to recognize that people have a specific right to know social media algorithms. Recognition of that specific right comports with the interest theory of rights, which justifies a legal right on the basis of the public interests it protects.[121] According to the theory, personal and collective interests—such as those concerning property, privacy, democratic participation, and communal safety—give rise to legal rights, imposing a duty on others to respect those rights.[122]

#### 1. Algorithmic Democratic Participation

The algorithms created and employed by social media companies, particularly recommendation algorithms, have an impact on the public interest regarding democratic participation. Social media companies use recommendation algorithms to sift through large volumes of content and present it to users in a manner that maximizes their attention. This automated service promotes news or other content based on various user-related factors, such as demographics, previous engagement history on the platform, or the behavior of the user's family or social network.[123] Recommendation algorithms can be divided into three main categories according to the filtering method they employ.

---

[118] AUSTRALIAN OFFICE OF MULTICULTURAL AFFAIRS, ACHIEVING ACCESS AND EQUITY, A SECOND EDITION GUIDE FOR THE AUSTRALIAN PUBLIC SERVICE (1994).

[119] *See id.*

[120] *See id.*

[121] JOSEPH RAZ, THE MORALITY OF FREEDOM 166 (1986).

[122] *See id.*

[123] Botambu Collins et al., *Trends in Combatting Fake News on Social Media—A Survey*, 5 J. INFO. & TELECOMM. 247, 250 (2021).

First, they can use collaborative filtering, which identifies the preferences of a large group of users and then recommends content based on the "underlying intuition . . . that if users A and B have similar taste in a product, then A and B are likely to have similar taste in other products as well."[124] Second, recommendation algorithms can employ content-based filtering. These algorithms focus more specifically on the preferences and history of the individual user being targeted, recommending content in which he or she has previously demonstrated interest.[125] Third, recommendation algorithms can employ hybrid systems, which use elements of both collaborative and content-based filtering, either by providing inputs to multiple algorithms in parallel and combining the results or by providing inputs to a single algorithm before passing on the output to further systems in sequence.[126]

Owing to these technical features, recommendation algorithms exert a huge impact on social media users' ability to participate in the democratic process. Most directly and significantly, recommendation algorithms can suppress certain kinds of speech because they determine the order in which content appears in users' feeds. They do so by processing data on a user's behavior, including "explicit feedback such as rating, following or subscribing, as well as implicit feedback such as scrolling and clicking." [127] In pursuit of increased user engagement and the maximization of advertising profits, recommendation algorithms frequently curtail the free exchange of ideas by promoting or relegating content "in ad hoc, automatic and opaque ways."[128] They can suppress some ideas "in unpredictable and undisclosed ways"[129] through technical functioning that is pre-determined by social media companies without any government intervention or public scrutiny. Worse still, such suppression is often unnoticed by users. It routinely occurs on the audience side of speech rather than the speaker side. Speakers remain free to post content, but the reach of their content is largely determined by recommendation algorithms operating in a black-box manner.[130]

Such suppression effected by recommendation algorithms thus affects the ability of speech audiences to participate democratically by configuring audiences into groups of people that are less capable of achieving democratic self-governance and engaging in the collaborative production of culture. Democratic self-governance involves participation in the formation of public

---

[124] Vatsal, *Recommender Systems Explained*, TOWARDS DATA SCIEUCE ( July 12, 2021), https://towardsdatascience.com/recommendation-systems-explained-a42fc60591ed [https://perma.cc/AW4R-ZXZ2].

[125] *Id.*

[126] *Id.*

[127] *See* Paddy Leersen, *The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems*, 11 E.J.LT. 1, 3-4 (2020).

[128] Kai Riemer & Sandra Peter, *Algorithmic Audiencing: Why we Need to Rethink Free Speech on Social Media*, 36 J. IuFO. TECH. 409, 410, 416-17 (2021).

[129] *Id.*

[130] *Id.*

opinion,[131] but this opportunity is denied if algorithms do not present a platform user's online speech to an audience. In a 2014 example, it was claimed that Facebook's prioritization of virality had led to users missing posts about protests pivotal to the formation of the Black Lives Matter movement in favor of the so-called Ice Bucket Challenge unless they had changed their settings to present content chronologically.[132]

The notion of autonomy in the digital age similarly involves participation, albeit in the formation of culture rather than opinion, and expressly requires a right to reach an audience.[133] Online communication is "interaction, sharing, influencing, and being influenced in turn," and creation involves building on the work of others and vice versa until, ultimately, "development of the self is a project that one shares with others."[134]

As recommendation algorithms tend to "favor nodes with high in-degree,"[135] meaning popular nodes with a large number of connections to other nodes in the network, they often reinforce pre-existing social biases, a potential consequence of which is that speakers from minority groups receive comparatively small audiences. Distorting the visibility of minorities can have a wide range of social consequences such as discouraging minority speech or encouraging minority speakers to exit online communities entirely.[136] These effects are extremely damaging to online expression, as certain voices lose the opportunity to participate in the formation of public opinion and culture in a society in which they are already underrepresented. Outside minority groups, there exists a general threat of invisibility for content that is not considered sufficiently important by recommendation algorithms.[137] A lack of visibility is so likely on social media that an entire news feed optimization industry has emerged to help brands boost their online presence.[138] A lack of visibility can also affect the discovery of truth through the marketplace of ideas. For example, vaccine and public health advocates have struggled to be heard in the face of competition from proponents of anti-vaccination conspiracies and falsehoods, who "have spent more than a decade building audiences and developing strategies that ensure they appear high in search results and automated recommendations."[139]

---

[131] *See supra* notes 91-105 and the accompanying text.

[132] *See* Riemer & Peter, *supra* note 128, at 416.

[133] *See* Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of. Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 43 (2004).

[134] *Id.*

[135] Fariba Karimi et al., *Minorities in Networks and Algorithms* 8 ( June 14, 2022) (unpublished manuscript), https://arxiv.org/abs/2206.07113 [https://perma.cc/MHA6-25M7].

[136] *Id.* at 4.

[137] Taina Bucher, *Want to be on the Top? Algorithmic Power and the Threat of Invisibility on Facebook*, 14 NEW MEDIA & SOC'Y 1164, 1171 (2012).

[138] *Id.*

[139] Brandy Zadrozny, *Drowned Out by the Algorithm: Vaccination Advocates Struggle to be Heard Online*, NBC NEWS (Feb. 27, 2019), https://www.nbcnews.com/tech/tech-news/drowned-out-algorithm-pro-vaccination-advocates-struggle-be-heard-online-n976321 [https://perma.cc/P98A-CH6P].

While some ideas or voices are unduly suppressed, others are unduly amplified. The profit maximization goal of recommendation algorithms often results in the promotion of irresponsible or harmful content. For instance, it has been argued that optimizing social media algorithms for engagement "all too often means optimizing for outrage, for polarization."[140] Under certain conditions, the amplification of hate speech can produce very real physical consequences.[141]

Recommendation algorithms are also capable of more subliminal impacts on individual autonomy. When platforms employ algorithms to make decisions about users, they are constructing users' digital identities and lumping them into digital categories created by the algorithms.[142] In the case of recommendation algorithms, a user's digital category determines the content to which he or she is exposed, thereby denying users the liberty to decide for themselves. However, the construction of a digital identity can also render users vulnerable to manipulation.[143] For instance, by presenting users with content they consider agreeable to maximize the time they spend using platform services, recommendation algorithms can create "filter bubbles" that isolate users from opposing views.[144] The end result is that users may unconsciously become convinced that their own political "bubbles" are representative, with a strong tendency to believe information that confirms their pre-existing beliefs at the expense of information that does not,[145] further limiting liberty to shape the self.

The amplification of disinformation by recommendation algorithms highlights their ability to shape user beliefs through filter bubbles. Unlike echo chambers, which are highly personalized information environments re- sulting from users' choices to follow like-minded individuals, filter bubbles are created covertly by platform algorithms that analyze individual user prefer- ences and tailor recommendations accordingly.[146] These algorithms can distort social capital, encompassing our connections to others and, most notably, "the level of trust (and trustworthiness) and the informal rules and common un-

---

[140] Jon Evans, *Facebook isn't Free Speech, it's Algorithmic Amplification Optimized for Outrage*, TECHCRUUCH (Oct. 20, 2019), https://techcrunch.com/2019/10/20/facebook-isnt-free-speech-its-algorithmic-amplification-optimized-for-outrage [https://perma.cc/Z99Q-HU8J].

[141] *See* Dan Milmo, *Rohingya Sue Facebook for £150bn Over Myanmar Genocide*, THE GUARDIAU (Dec. 6, 2021), https://www.theguardian.com/technology/2021/dec/06/rohingya-sue-facebook-myanmar-genocide-us-uk-legal-action-social-media-violence [https://perma.cc/FM32-JPMH].

[142] Balkin, *Free Speech in the Algorithmic Society*, *supra* note 1, at 1164, 1167.

[143] *Id.*

[144] Samuel C. Rhodes, *Filter Bubbles, Echo Chambers, and Fake News: How Social Media Conditions Individuals to Be Less Critical of Political Misinformation*, 39 POL. COMM. 1, 6 (2022).

[145] ELISABETH COSTA & DAVID HALPERU, THE BEHAVIOURAL IUSIGHTS TEAM, THE BEHAVIOURAL SCIEUCE OF OULIUE HARM AUD MAUIPULATIOU, AUD WHAT TO DO ABOUT IT: AU EXPLORATORY PAPER TO SPARK IDEAS AUD DEBATE (Apr. 15, 2019), https://www.bi.team/wp-content/uploads/2019/04/BIT_The-behavioural-science-of-online-harm-and-manipulation-and-what-to-do-about-it_Single.pdf [https://perma.cc/CPY8-5K2M].

[146] Rhodes, *supra* note 144, at 4-5.

derstandings that facilitate communication."[147] Filter bubbles deceive us into thinking that our social and political "bubbles" are representative.[148] Furthermore, they promote confirmation bias, as humans inherently trust familiar sources that align with their existing worldview.[149] Social media platforms that amplify disinformation can be especially problematic, as studies indicate that people are more prone to accept information when engaging with it passively, as in the case of social media.[150]

2. Algorithmic Public Safety

Social media algorithms are also closely related to a myriad of interests in maintaining and improving public safety, ranging from protection of the media environment to data security preventing the unauthorized leakage of data to a third party or the public to health matters. For example, the impact of "fake news" can be to promote such emotions as fear, doubt, and anger,[151] generating "clicks, shares, and social engagements" as a consequence.[152] Algorithmic amplification challenges the marketplace of ideas metaphor, as the mass, targeted dissemination of false information on social media can overwhelm users and prevent the "truth" from rising to the top.[153]

Content moderation algorithms can easily spread and amplify fake news. One way in which they do so is by prioritizing the promotion of content aligned with a social media company's platform policy over content that users might be most interested in. For instance, in one of its earlier forms, Facebook's algorithm was designed to recommend content that attracted a large number of likes and clicks. Once it was discovered that the design had led to a rise in clickbait, the algorithm target was changed to content that users spent the most time consuming.[154] Then, after realizing that users were consuming content passively and increasingly taking more active forms of communication to other platforms, Facebook again redesigned its algorithm to target "meaningful social interactions" by amplifying posts that sparked a lot of comments and replies. In reality, this was often because those posts had offended or angered users.[155] Facebook has reportedly conducted multiple studies indicating that the types of content most likely to promote engagement in the form of comments and replies can be considered harmful, such as politically divisive

---

147 *See* COSTA & HALPERU, *supra* note 145, at 24.

148 *Id.*

149 *See* Rhodes, *supra* note 144, at 6.

150 *Id.*

151 GIAUSIRACUSA, *supra* note 40, at 79.

152 Ari Ezra Waldman, *The Marketplace of Fake News*, 20 J. COUST. L. 845, 858 (2018).

153 *See* Daniela C. Manzi, *Managing the Misinformation Marketplace: The First Amendment and the Fight Against Fake News*, 87 FORDHAM L. REV. 2623, 2628 (2019).

154 Will Oremus et al., *How Facebook Shapes Your Feed*, WASH. POST (Oct. 26, 2021), https://www.washingtonpost.com/technology/interactive/2021/how-facebook-algorithm-works [https://perma.cc/SY4X-LVCG].

155 *Id.*

speech and misinformation.[156] Nevertheless, Facebook has continued using this algorithm, even pushing pages with "engaging" content onto the feeds of users who do not follow those pages.[157] This dynamic has been exploited by troll farms, which create fake news stories specifically designed to generate engagement so that the algorithm amplifies the content, in turn generating more clicks and thus ad revenue.[158]

Powered by technologies such as deep learning, recommendation algorithms have grown increasingly complex, with potentially negative consequences. Following a recent major policy change, YouTube shifted focus away from video clicks toward watch time.[159] Taken at face value, the policy change appears to benefit users, as they are recommended videos that others are watching at length. Then, in 2015, YouTube developed a new algorithm incorporating deep learning technology to narrow down a vast pool of potential recommendations to a few hundred based on a user's "watched video history, keyword search history . . . the geographic region the user is logged in from, the type of device they are using, and the user's age and gender if they have provided that information," ranked according to user-specific predictors, as well as "a few hundred video-specific predictors, including details on the user's previous interactions with the channel the video is from."[160] The algorithm demotes a video each time it is recommended to a user but not clicked on.[161] The technology developed further in 2018 when YouTube introduced a deep reinforcement learning model designed to predict how long a user might spend watching the next recommended video, the aim being to hook the user into viewing a succession of videos.[162] The algorithm operates through a re- ward function based on "something like the total amount of watch time each user spends in a sequence of up next recommendations before leaving the site."[163] The algorithm thus encourages recommendations that may not initial- ly generate much watch time but expose the user to a whole new topic or category of content, potentially leading to him or her remaining active for longer than if he or she had consumed only familiar content.[164]

These advanced algorithmic designs have made fake news an endemic problem on YouTube. After a rise in the popularity of far-right politicians in Brazil, for example, a 2019 Harvard study conducted for *7e New York Times* found that following the chain of top recommendations from a video on a

---

156 Karen Hao, *Troll Farms Reached 140 million Americans a Month on Facebook Before 2020 Election, Internal Report Shows*, MIT TECH. REV. (Sept. 16, 2021), https://www.technologyreview.com/2021/09/16/1035851/facebook-troll-farms-report-us-2020-election [https://perma.cc/NH6F-2TCA].

157 *Id.*

158 *Id.*

159 *See* GIAuSIRACUSA, *supra* note 40, at 71.

160 *Id.* at 73.

161 *Id.*

162 *Id.* at 75.

163 *Id.*

164 *Id.*

popular channel unrelated to politics often led to videos on right-wing, conspiracy-filled channels, including that of ex-president Jair Bolsonaro.[165] In a similar manner to Facebook, this effect is credited to the YouTube algorithm's emphasis on watch time, as "fear, doubt, and anger . . . the same emotions that right-wing extremists and conspiracy theorists have relied on for years . . . draw people in to content and keep them tuned in."[166] In 2016, an engineer who had previously worked on YouTube's recommendation algorithm team designed a computer program to track where the platform would take a user from seed videos discovered after making what the engineer considered to be common or important searches relating to the U.S. presidential election.[167] His findings suggested that divisive, sensational, and conspiratorial content was systematically amplified by the platform, with a search for "Who is Mi- chelle Obama?" leading to videos falsely claiming that she was a man.[168]

Falsehoods diffuse "significantly farther, faster, deeper, and more broadly than the truth in all categories of information" on social media.[169] According to a study looking at diffusion through retweets and the independent tweeting of true, false, and mixed rumors, the veracity of which were agreed upon by six independent fact-checking organizations,[170] the truth took about six times as long as falsehoods to reach 1500 people.[171] The study did not look specifically at the role of recommendation algorithms in structuring the presentation of content, but explained the difference in speed as a consequence of human behavioral tendencies, noting that false news evokes emotion and is more novel, and "novel information is more likely to be retweeted."[172] Nevertheless, commentators have highlighted the importance of engagement to recommendation algorithms, suggesting that the study demonstrates the dangers of such an algorithmic approach.[173] If false information is more likely to generate emotional reactions and retweets than true information, then there is a possibility

---

[165] *Id.* at 77; *See, e.g.,* Max Fisher & Amanda Taub, *How YouTube Radicalized Brazil*, N.Y. TIMES (Apr. 11, 2019), https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html [https://perma.cc/HC33-N8YZ].

[166] *See* GIAUSIRACUSA, *supra* note 40, at 79.

[167] *Id.* at 86.

[168] *Id.*

[169] Soroush Vosoughi et al., *The Spread of True and False News Online*, 359 SCIENCE 1146, 1147 (2018).

[170] *Id.* at 1146 ("Here we investigate the differential diffusion of true, false, and mixed (partially true, partially false) news stories using a comprehensive data set of all of the fact-checked rumor cascades that spread on Twitter from its inception in 2006 to 2017. The data include ~126,000 rumor cascades spread by ~3 million people more than 4.5 million times.").

[171] *Id.* at 1148.

[172] *Id.* at 1147-48.

[173] Robinson Meyer, *The Grim Conclusions of the Largest-Ever Study of Fake News*, THE ATLANTIC (Mar. 8, 2018), https://www.theatlantic.com/technology/archive/2018/03/largest- study-ever-fake-news-mit-twitter/555104 [https://perma.cc/W62P-L9KQ] ("Tromble, the political-science professor, said that the findings would likely apply to Facebook, too. 'Earlier this year, Facebook announced that it would restructure its News Feed to favor "meaningful interac- tion," she told me. 'It became clear that they would gauge "meaningful interaction" based on the number of comments and replies to comments a post receives. But, as this study shows, that only

that Twitter's algorithm has played a role in recommending tweets containing false rumors or a risk that it will do so in the future.

Social media platforms' collection and utilization of personal data through their algorithms pose serious treats to data security for the entire society.[174] Their personalization service is sustained by a set of algorithmic codes performing a ranking and classification system.[175] Despite being widely utilized, the algorithmic personalization service by itself is not profitable. According to Shoshana Zuboff, Google, the pioneer of the personalization service, suffered a severe financial crisis in 1999.[176] The situation suddenly changed when Google started to generate ads from search queries.[177] The key to Google's success is to sell the personalization system not to users but to advertisers. In today's world, various platforms gain substantial profits by allowing advertisers to deliver personalized ads to particular segments of users.[178]

The economic motive underlying the algorithm-driven personalization service incentivizes social media platforms to harvest a large amount of information about users.[179] Three "vs" of datasets directly determine the accuracy of algorithmic output: volume (i.e., the size of the dataset), variety (i.e., the type of data), and velocity (i.e., rate of flow).[180] High-volume, high-variety, and high-velocity datasets produce reliable and accurate profiles of users' behaviors, preferences, and emotions. The more accurate the personalization is, the greater profits it brings to social media platforms. Interested buyers include but are not limited to advertisers, insurance companies, and political consultant firms.

For this reason, social media platforms are eager to reap every bit of personal data through various channels, such as using online and offline trackers

---

further incentivizes creating posts full of disinformation and other content likely to garner strong emotional reactions,' she added.").

174 PASQUALE, *supra* note 5, at 4 ("Internet companies collect more and more data on their users but fight regulations that would let them same users exercise some control over the resulting digital dossiers.").

175 Jan Dwivedi-Yu et al., *A$ective Signals in a Social Media Recommender System*, *in* PROCEEDIugS OF THE EITH ACM SIGKDD COuFEREuCE Ou KuOwlEDGE DISCOVERY AuD DATA MIuIug EIFi (2022), https://doi.org/10.1145/3534678.3539054 [https://perma.cc/T85H- JL7K].

176 SHOSHAuA ZUBOFF, THE AgE OF SURVEILLAuCE CAPITALISM: THE FIGHT FOR A HUmAu FUTURE AT THE NEw FROuTIER OF POwER 71 (2019).

177 *Id*. at 72.

178 Paul Hitlin et al., *Facebook Algorithms and Personal Data*, PEw RSCH. CTR. ( Jan. 16, 2019), https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data [https://perma.cc/SP7Y-EMNS].

179 Ari Waldman & Kirsten Martin, *Governing Algorithmic Decisions: 7e Role of Decision Importance and Governance on Perceived Legitimacy of Algorithmic Decisions*, 9 BIG DATA & SOC'Y 1, 2 (2022) ("Algorithmic systems also incent surveillance and data collection because they need large information sets for model training and analysis").

180 NAT'l IuST. OF STAuDARDS & TECH. BIG DATA PUB. WORKIug GRP., U.S. DEP'T OF COM., NIST BIG DATA IuTEROPERABILITY FRAMEwORK: VOLUME i, DEFIuITIOuS (2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-1r2.pdf [https://perma.cc/D8KQ-C5MK].

or purchasing datasets from data brokers.[181] Data collection through social media platforms is ubiquitous and unprecedented. Facebook's personality quiz app, This Is Your Digital Life, is a good example. According to court documents in Australia, "[o]nly 53 people in Australia installed the This is Your Digital Life app but it was able to harvest the data of about 311,127 people."[182] It has also been reported recently that this app grasped direct messages between Facebook users without their express consent.[183]

Data collection on this scale causes privacy harm. Users believed that This Is Your Digital Life was a psychology quiz app that would only gather data about their answers. They were unaware that the app was collecting personal data, and they had no say on who could access this personal data on Facebook. Danielle Citron and Daniel Solove refer to this phenomenon as a "thwarted expectation," which negatively impacts individuals' autonomy in managing their privacy.[184] In other words, when platforms fail to keep their promises regarding data collection, they undermine people's ability to make informed choices.

A Pew Research Center survey revealed that 51% of respondents felt uneasy upon discovering how Facebook categorized them.[185] This discomfort among Facebook users highlights potential breaches of personal data. As Samuel Warren and Louis Brandeis argued, an "injury to the feelings" is legally cognizable harm in U.S. common law.[186] The Pew Research Centre survey also showed that 27% of respondents believed Facebook had inaccurately classified them.[187] The inaccuracy of algorithmic classification, if connected to one's identity, can cause reputational harm. Imagine, for example, Facebook algorithms mistakenly classifying a U.S. citizen, Zach, as a user who regularly spreads terrorist and extremist content.[188] After Facebook shares datasets with

---

[181] *Data Brokers: A Call For Transparency and Accountability*, FED. TRADE COMM'u (May 2014), https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014 [https://perma.cc/S6G8-NBT7].

[182] *See* Christopher Knans, *Facebook Appeal over Cambridge Analytica Data Rejected by Australian Court as "Divorced from Reality,"* THE GUARDIAu (Feb. 6, 2022), https://www.theguardian.com/technology/2022/feb/07/facebook-appeal-over-cambridge-analytica-data-rejected-by-australian-court-as-divorced-from-reality [https://perma.cc/AKU8-PG8A].

[183] Alex Hern & Carole Cadwalladr, *Revealed: Aleksandr Kogan Collected Facebook Users' Direct Messages*, THE GUARDIAu (Feb. 6, 2022), https://www.theguardian.com/uk-news/2018/apr/13/revealed-aleksandr-kogan-collected-facebook-users-direct-messages [https://perma.cc/4KNR-ANGR].

[184] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 BOSTOu U. L. REV. 793, 849 (2022).

[185] Hitlin et al., *supra* note 178.

[186] Samuel D. Warren & Louis D. Brandeis, *7e Right to Privacy*, 4 HARV. L. REV. 193, 197-98 (1890).

[187] Hitlin et al., *supra* note 178.

[188] *Facebook, Microsoft, Twitter, and YouTube Announce Formation of the Global Internet Forum to Counter Terrorism*, META ( June 26, 2017), https://about.fb.com/news/2017/06/global-internet-forum-to-counter-terrorism [https://perma.cc/7A9T-DL76].

U.S. Customs, Zach is always delayed before boarding, and is never informed by authorities that he is suspicious because of his Facebook profile.

3. Algorithmic Social Equality

Social media algorithms greatly affect public interest in the promotion of social equality. The notion that neutral algorithms rate all individuals in the same way is inaccurate. It is human developers who design the core elements of algorithmic operations, ranging from the data-mining process to predictive models to decision trees.[189] Consequently, human biases are embedded in virtually every stage of an algorithmic decision-making system's construction.[190] Moreover, the algorithms used in machine learning systems often "produce results that reflect the prejudices of society"[191] because they adapt to inputs generated by their users and optimize search engine results or recommend engaging content on social media. For instance, the autocomplete function of Google's search engine was called to task in a UN Women ad campaign for completing the prompt "women should" with such phrases as "stay at home," "be slaves," and "be in the kitchen."[192]

The prioritization of certain kinds of user engagement in social media algorithms can lead to the promotion of incendiary, often racist, content.[193] In one case study in Australia, an indigenous football player was subjected to online harassment after celebrating a goal with a traditional dance, ultimately leading to him quitting both football and social media.[194] The study found that images, videos, posts, and comments on social media had amplified the racist discourse surrounding the player and that algorithms had played an im- portant role in such amplification.[195] As an example, it cited a video shared on Twitter in which the wife of one of the player's indigenous teammates praised the player as a good role model for her future children.[196] The first comment under the shared video, there by virtue of its 2,222 likes, said "Racism goes both ways your kids won't be Indigenous. They will be Australian. Stop segregating."[197] Although not an overtly racist post, it denied the Aboriginal heri-

---

189 PASQUALE, *supra* note 5, at at 25 ("[C]onstruct the datasets mined by scoring systems; they define the parameters of data-mining analyses; they create the clusters, links, and decision trees applied; they generate the predictive models applied.").

190 *Id.* (arguing that ensuring scope for human biases to become "embedded into each and every step of development").

191 *See* Chander, *supra* note 11, at 1036.

192 *Id*. at 1034-36.

193 *See id.*

194 Ariadna Matamoros-Fernández, *Platformed Racism: 7e Mediation and Circulation of an Australian Race-Based Controversy on Twitter, Facebook and YouTube*, 20 COMM. & SOC'Y 930, 931 (2017).

195 *Id.* at 938.

196 *Id.*

197 *Id.*

tage of the woman's future children and minimized the historic segregation of indigenous peoples during the colonization of Australia.[198]

On social media, both underlying data and real-time user inputs can generate discriminatory results through the creation of user profiles. Social media user profiles usually incorporate demographic information such as users' age, location, and education level, as well as their interests and preferences inferred from their platform behavior, including likes, clicks, and time spent reading posts.[199] However, using data to draw inferences about individuals is a pervasive and challenging source of algorithmic discrimination. Widespread data mining and brokering offer algorithms access to all kinds of inferences. For instance, a person's health status might be inferred from his or her use of a mobile weight-tracking device, but it might also be inferred from Amazon data on the purchase of a diet book, search engine queries about diabetes, or a brokered dataset integrating all of these sources.[200] Once data are used to draw negative inferences, and disfavor or differential treatment ensues, the door is opened to discrimination.[201]

No matter how benign an algorithm's underlying data may appear, individuals can be subjected to racial discrimination based upon negative inferences drawn from that data. For instance, even when race is specifically excluded from data in an attempt to ensure neutrality, other characteristics may still serve as a proxy for the missing information.[202] Given the technical nature of machine learning, social media platforms using algorithms that draw upon user profiles and inferences to decide what forms of content to promote, and whom to promote them to, face a difficult task in avoiding proxy discrimination. Machine learning systems are designed to automate the discovery of useful patterns in data for the purpose of generating a target outcome and to ignore potential explanations for those patterns, as they are immaterial to the discovery task.[203] Depriving the systems of such characteristics as race will not prevent unintentional proxy discrimination, as they will use "brute force" to determine which characteristics correspond with particular outcomes, and will use data to derive "proxies for directly predictive characteristics when they are deprived of direct data on these characteristics."[204] For example, excluding race as an input to an algorithm designed to review an applicant's suitability for a loan will not prevent disproportionately negative outcomes for minority applicants, as the

---

198 *Id.*

199 Engin Bozdag, *Bias in Algorithmic Filtering and Personalization*, 15 ETHICS IuF. TECH. 209, 213 (2013).

200 *See* PASQUALE, *supra* note 5, at 31.

201 *Id.* at 38.

202 Anya Prince & Daniel Schwartz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 IOWA L. REV. 1257 (2020).

203 *Id.* at 1273-74.

204 *Id.* at 1274-75.

system might decide that applicants from certain zip codes, particularly those "predominantly composed of a particular race or ethnicity," are not good bets.[205]

In the social media context, ostensibly innocuous activities can act as proxies for race.[206] For instance, one study exploring Facebook "likes" found that white Americans and African Americans could be identified correctly in 95% of cases based solely on the pages they had liked.[207] Algorithms used in targeted advertising, a prominent feature of social media platforms, have also been found to lead to proxy discrimination. African American-sounding names, for example, were found to generate more advertisements relating to arrest records than names typically associated with white Americans.[208]

The treatment of social media algorithms as commercial secrets makes it extremely difficult to properly address algorithmic discrimination. Most fundamentally, the existence of algorithm secrecy makes it "impossible to know exactly what's going on."[209] It is difficult for accountability to be achieved if algorithm designs and processes, including the design measures introduced to counter discrimination, are kept secret. Even if platforms publicize anti-discrimination policies and initiatives, the public has no proof that they are not simply performative or underfunded, as industry insiders have suggested.[210] Given the role of data and data-based inferences in generating discriminatory outcomes, and the black box nature of algorithm design, mandating transparency for input data, rather than algorithms themselves, would likely be more effective in addressing algorithm-generated discrimination and holding platforms accountable.[211] However, as underlying data can also be treated as trade secrets,[212] both approaches are currently obstructed by the culture of secrecy that surrounds social media algorithms.

---

[205] Lance Eliot, *Insidious AI-Based Proxy Discrimination Against Humans Is Dauntingly Vexing For AI Ethics, Which Can Occur Even In The Case Of Autonomous AI Self-Driving Cars*, FORBES (Apr. 8, 2022), https://www.forbes.com/sites/lanceeliot/2022/04/08/insidious-ai-based-proxy-discrimination-against-humans-is-dauntingly-vexing-for-ai-ethics-which-can-occur-even-in-the-case-of-autonomous-ai-self-driving-cars/?sh=3a2427cc6b7b [https://perma.cc/6AVZ-VBXN].

[206] *See* Chander, *supra* note 11, at 1038.

[207] Michal Kosinski et al., *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 PROC. NAT'L ACAD. OF SCI. 5802, 5803 (2013).

[208] *See* Chander, *supra* note 11, at 1037.

[209] *See* PASQUALE, *supra* note 5, at 39.

[210] Ashely Marie Preston, *Taking On Tech: Social Media's Anti-Blackness And Algorithmic Aggression In The Absence Of Accountability*, FORBES (Aug. 9, 2021), https://www.forbes.com/sites/forbestheculture/2021/08/09/taking-on-tech-social-medias-anti-blackness-and-algorithmic-aggression-in-the-absence-of-accountability/?sh=1bb901963c79 [https://perma.cc/8QBR-XBND].

[211] *See* Chander, *supra* note 11, at 1039-44.

[212] *See* Deven R. Desai & Joshua A. Kroll, *Trust but Verify: A Guide to Algorithms and the Law*, 31 HARV. J.L. & TECH. 1, 56 (2017).

## III. WHY THE RIGHT TO KNOW COULD PREVAIL OVER ALGORITHMIC SECRECY

As Part I has shown, trade secrets and social media algorithms are private property belonging to their respective companies. One might thus argue that the public's right to know algorithms should not necessarily supersede the trade secret rights held by social media companies. Recall that among its nine disclosure exemptions, the FOIA allows a government agency to choose not to disclose trade secrets collected from a person.[213] This exemption could arguably apply to social media companies, exempting them from disclosing their algorithms that are protected as trade secrets. However, the argument does not hold because that FOIA exemption merely prevents the government from disclosing trade secrets without the consent of the rights owner. The government is not the rights owner of the trade secrets they collect.

However, social media companies are in a different position. As the rights owners of their algorithms, they could appropriately disclose information about their algorithms for the purpose of meeting certain regulatory or public policy mandates. In this part, I examine why the public policy considerations gleaned from the right to know could empower this legal right to prevail over trade secret rights concerning social media algorithms.

### A. *Dealing with Algorithmic Secrecy's Social Harms*

Social media platforms, by their very nature, are private companies providing commercial services. Consequently, individual users have little grounds to demand or expect disclosure of information about a platform' algorithms.[214] This protection of algorithms as trade secrets further reinforces the notion that private commercial ownership allows platforms to control information without providing transparency or communication about the underlying processes and systems in play.

On the other hand, social media platforms have amassed significant control over how information is disseminated. Despite numerous instances of irresponsible management of this control, society has been compelled to accept the unchecked power wielded by these platforms passively. Nearly two-thirds of Americans now obtain at least part of their news from social media. However, it is the commercial interests of social media companies, through engagement-driven algorithms or paid advertisements, that determine what users see.[215]

However, safeguarding algorithms as trade secrets has enabled platforms to exert control over our access to knowledge, leading to widespread informa-

---

[213] Freedom of Information Act, 5 U.S.C § 552 (b) (4) ("This section does not apply to matters that are . . . trade secrets and commercial or financial information obtained from a person and privileged or confidential. ").

[214] *Id.*

[215] Kalev Leetaru, *The Algorithms Are Taking Over: Who Controls Our Online Future?*, FORBES ( Jan. 2, 2016), https://www.forbes.com/sites/kalevleetaru/2016/01/02/the-algorithms-are-taking-over-who-controls-our-online-future/?sh=4e0f3bed22b0 [https://perma.cc/DA9Z-397L].

tion disorder in the era of social media. This disorder can arise from flawed practices and errors in both algorithmic and human moderation processes. For example, Mark Zuckerberg contends that Facebook effectively removes explicit and hateful content given its billions of users, whereas critics argue that the platform consistently makes mistakes, sometimes with dire consequences.[216]

Content recommendation is also a source of information disorder. Although many perceive algorithmic recommendations as well-controlled or personalized, the reality is often far more disordered.[217] First, machine learning processes such as recommendation algorithms consist of various processes, techniques, data, and outputs "working together as a system."[218] Although each component offers the possibility of some degree of control, it can be difficult to maintain control of the overall system.[219] A well-designed and accurate system can become obsolete when applied in the real world owing to the inputs it encounters, with Microsoft's benign Twitter bot Tay, for example, becoming foul-mouthed and racist after being fed data by Twitter trolls.[220] Second, personalization may be simply inaccurate. Recommendation algorithms are prediction engines designed to create and refine a theory of who a user is and what he or she will want to see next but, ultimately, any theory is based on a combination of information gathered, approximated, and excluded because the system deems it unimportant.[221]

Although the scale of social media platforms means that moderation and recommendation mistakes are inevitable, it is "the use of automated review mechanisms, the limited contact options, and the lack of an appeals process," as well as the general lack of communication or transparency, that is problematic and "a growing hallmark of the digital world."[222] Worse, society is also being forced to watch recommendation-generated information disorder unfold in the real world.

For instance, content promotion on social media plays a major role in the legitimization of inaccurate beliefs. Many social media users seek out and consume information that affirms their sense of self, regardless of inaccuracies in the content.[223] When this tendency is combined with algorithmic distortion and restriction, whether unintentional or in pursuit of some platform goal, "our window to the world becomes a slit."[224] Moreover, human beings are

---

[216] Danny O'Brien, *Can Algorithms Pose a Threat to Free Speech?*, DIGITAL FUTURE SOC'Y (Apr. 21, 2021), https://digitalfuturesociety.com/qanda/can-algorithms-pose-a-threat-to-free-speech/[ https://perma.cc/7KVR-ZXS6].

[217] Desai & Kroll, *supra* note 212, at 21.

[218] *Id.*

[219] *Id.*

[220] *Id.*

[221] Henrik Skaug Sætra, *The Tyranny of Perceived Opinion: Freedom and Information in the Era of Big Data*, 59 TECH. SOC'Y 1, 6-7 (2019).

[222] *See* Leetaru, *supra* note 215.

[223] Geoffrey Baym, *Is There a Cure for Information Disorder?*, JSTOR DAILY (Nov. 3, 2022), https://daily.jstor.org/is-there-a-cure-for-information-disorder/ [https://perma.cc/7659-UEUY ].

[224] *See* Sætra, *supra* note 221, at 6.

more susceptible to misinformation that is consistent with their world views or social identities.[225] Algorithms can reinforce such susceptibility by adding "an air of legitimacy" to conspiracy theories and false information.[226] Recommendation algorithms can also promote hateful and obscene content. For instance, as Facebook's "feed" is driven by engagement, polarizing and incendiary posts that invoke strong emotional reactions rise to the top.[227]

We may rely on traditional exceptions to trade secret protection to deal with social harms caused by algorithmic secrecy. After all, trade secret rights are not absolute rights. The law allows for the unauthorized disclosure of trade secrets when there are valid public policy grounds that prevail over the private interests in those secrets.[228] For example, some state and federal whistleblower statutes "privilege disclosures that might otherwise be regarded as trade secret misappropriations."[229] The Defend Trade Secrets Act also introduced new whistleblower provisions to protect employees who disclose trade secrets to specified individuals "in confidence" to bring illegal activity to public attention.[230]

Although those traditional exceptions provide a check on the potential for absolute protection of trade secrets, the technical inscrutability of algorithms undermines those doctrines' effectiveness. First, modern-day trade secrets such as algorithms can be extremely resilient to reverse engineering.[231] In contrast to physical inventions, algorithms can be easily shielded from public access.[232] Competitors can observe the decisions made by platform algorithms but, owing to their inscrutability and unpredictability, the results are extremely difficult to replicate. Second, as algorithms automate responsibilities, they reduce the need for human employees, who in other industries might take their

---

[225] Richard Sima, *Why do our Brains Believe Lies?*, WASH. POST (Nov. 3, 2022), https://www.washingtonpost.com/wellness/2022/11/03/misinformation-brain-beliefs/ [https://perma.cc/2ATv-JP4Q].

[226] *See* GIAuSIRACUSA, *supra* note 40, at 80.

[227] Luke Munn, *Angry by Design: Toxic Communication and Technical Architectures*, *in* HUMAuITIES AuD SOCIAL SCIEuCE COMMUuICATIOuS 1, 3 (2020).

[228] *See* Charles Tait Graves & Sonia K. Katyal, *From Trade Secrecy to Seclusion*, 109 GEO. L.J. 1337, 1412 (2021) ("Trade secret protection should not be viewed as a monolith where the skimpiest satisfaction of the elements of trade secrecy means that regulatory or other disclosure in the public interest is impossible. There are contexts where the public interest in disclosure is strong, and the case for competitive harm is weak."); Katyal, *supra* note 14, at 140 (suggesting that "it is indeed possible to exploit the potential for whistleblower liability as a public policy exemption to encourage greater algorithmic transparency"); Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection*, 105 CAL. L. REV. 1, 61–62 (2017) (discussing public policy considerations for protecting whistleblowing activity); David S. Levine, *The People's Trade Secrets*, 18 MICH. TELECOMM. & TECH. L. REV. 61, 102-06 (2011).

[229] Pamela Samuelson, *Principles for Resolving Conflicts between Trade Secrets and the First Amendment*, 58 HASTIuGS L.J. 777, 788 (2007).

[230] Sharon K. Sandeen & Ulla-Maija Mylly, *Trade Secrets and the Right to Information: A Comparative Analysis of E.U. and U.S. Approaches to Freedom of Expression and Whistleblowing*, 21 N.C. J.L. & TECH. 1, 58 (2020).

[231] *See* Hrdy & Lemley, *supra* note 65, at 13.

[232] Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORuELL L. REV. 1183, 1216 (2019).

residual know-how to competitors.[233] A consequence of such indefinite protection is that information becomes trapped in the firm, shielded from both those who might be able to learn from it and members of the public with a valid and undeniable interest.[234] Technology can now advance in a matter of months, with new versions of platform algorithms introduced on a regular basis.[235] Yet even an outdated algorithm may never be seen by the public, "even after it has lost its commercial utility."[236] Such relentless and deliberate obfuscation is emblematic of the culture of secrecy surrounding social media algorithms.

Knowledge is power, and the freedom to "scrutinize others while avoiding scrutiny oneself is one of the most important forms of power."[237] Social media companies profit from the intimate details of their users' lives but offer no transparency in return and actively fight regulatory efforts to ensure the disclosure of information.[238] One of the tools used to enable and justify such conduct is the trade secret protection afforded to social media algorithms. Trade secret status is conditioned on the implementation of efforts to maintain secrecy, ensuring that the best available means of protecting social media algorithms from competitors actively discourage transparency.[239] Despite being developed to ensure commercial morality, trade secret protection now "clashes with the ability to know whether software is operating as it should and . . . can interfere with legal-political accountability."[240]

### B. *Generating New Public Policy Considerations*

Recognition of the right to know algorithms could provide new public policy considerations justifying the disclosure of trade secrets pertaining to social media algorithms on grounds of protecting democratic participation, public safety, and social equality. The culture of algorithm secrecy must be re-examined because algorithms are not simply secret recipes or formulas;

---

[233] Jeanne C. Fromer, *Machines as the New Oompa-Loompas: Trade Secrecy, the Cloud, Machine Learning, and Automation*, 94 N.Y.U. L. REV. 706, 725-26 (2019); *See* Hrdy & Lemley, *supra* note 65, at 13.

[234] *See* Hrdy & Lemley, *supra* note 65, at 14.

[235] *Id.* at 5-6; Digital marketing companies often publish advice on how to handle the frequency at which major algorithms change. *See, e.g.*, Aleksandra Stefanovic, *Why C How to Track Google Algorithm Updates*, PLAY MEDIA ( June 20, 2022), https://play-media.org/how-to-track-google-algorithm-updates [https://perma.cc/LN93-YC8U] ("Most experts estimate that Google changes its search algorithm around 500 to 600 times each year. That's somewhere between once and twice each day. While most of these changes don't significantly change the SEO landscape, some updates are significant."); *Instagram Algorithm 2022: How to Conquer it*, STATUSBREW (Sep. 7, 2021), https://statusbrew.com/insights/instagram-algorithm/ [https://perma.cc/9KTX-JRCD] ("Instagram is constantly evolving. . . However, that is not the only feature of Instagram that has changed. Recently, Instagram has introduced lots of improvements within the IG algorithm. It continues to curate and organize its feed to provide more relevant content to its users.").

[236] *See* Hrdy & Lemley, *supra* note 65, at 14-15.

[237] *See* PASQUALE, *supra* note 5, at 3.

[238] *Id.*

[239] *See* Foss-Solbrekk, *supra* note 70, at 257.

[240] *See* Desai & Kroll, *supra* note 212.

they are the architectural foundation of the modern-day information ecosystem.[241] The appropriate disclosure of algorithm trade secrets has the potential to avert the harm caused by platforms' mismanagement of the information ecosystem. Such potential is clear from the ever-growing list of harmful consequences that have been attributed to social media algorithms and platforms' failures to respond to warning signs.

For instance, TikTok's algorithms were accused in both the U.K. and U.S. of promoting the dangerous "blackout challenge" requiring users to choke themselves until they pass out and which has allegedly resulted in the death of children as young as eight.[242] However, irresponsible platforms are currently empowered to think only of the commercial aspects of their algorithms. In 2018, Facebook's own research found that its recommendation policies were feeding its users increasingly divisive content, but "Facebook management ignored these findings and shelved the research."[243] Requiring platforms to communicate such findings could instill a level of accountability that avoids such decisions and averts possible harm.

In perhaps the most explicit example of the need for greater algorithm transparency, civic leaders brought a lawsuit against Facebook in December 2021, claiming that its algorithm had amplified hate speech contributing to the 2017 genocide of Myanmar's Rohingya Muslim population.[244] Civic lead- ers in Myanmar claimed that social media platforms had been "pumping the national bloodstream with conspiracies and ultranationalist rage" and that Facebook had ignored multiple warnings about the rising tensions.[245] That Facebook had no Myanmar office from which to truly appreciate the dangers its algorithm was fueling[246] does not excuse Facebook. Instead, it provides compelling evidence of the need for its algorithm to be made more transparent. If Facebook cannot manage information effectively enough to prevent harm on such an unimaginable scale on the other side of the world, then it should be willing to accept that it requires external support.

As noted, social media algorithms can cause serious discrimination owing to the potential human biases embedded in them. Such discrimination is un-

---

[241] Marietje Schaake, *Trade Secrets Shouldn't Shield Tech Companies' Algorithms from Oversight*, BROOKIUGS (May 4, 2020), https://www.brookings.edu/techstream/trade-secrets-shouldnt-shield-tech-companies-algorithms-from-oversight [https://perma.cc/EUE9-JS7F].

[242] Michael Levenson & April Rubin, *Parents Sue TikTok, Saying Children Died After Viewing 'Blackout Challenge,'* N.Y. TIMES ( July 6, 2022), https://www.nytimes.com/2022/07/06/technology/tiktok-blackout-challenge-deaths.html [https://perma.cc/HQ7C-UA5M]; Kate Ng, *Archie Battersbee: What is the Dangerous Social Media 'Blackout' Challenge?*, THE IUDEPEU- DEUT (Aug. 8, 2022), https://www.independent.co.uk/life-style/archie-battersbee-whats-the-blackout-challenge-b2139497.html [https://perma.cc/RZG4-JD35].

[243] *See* Munn, *supra* note 227, at 4.

[244] Dan Milmo, *Rohingya Sue Facebook for £150bn Over Myanmar Genocide*, THE GUARDIAU (Dec. 6, 2021), https://www.theguardian.com/technology/2021/dec/06/rohingya-sue-facebook-myanmar-genocide-us-uk-legal-action-social-media-violence [https://perma.cc/7GHZ-TB2G].

[245] *See* MAX FISHER, THE CHAOS MACHIUE: THE IUSIDE STORY OF HOW SOCIAL MEDIA REWIRED OUR MIUDS AUD OUR WORLD 158 (2022).

[246] *Id.*

surprising given the persistence of racism, but it is unlikely this outcome is the intention of racist programmers or actively discriminatory platform policies.[247] Instead, algorithmic discrimination on social media is more likely the consequence of platforms' algorithms and flaws in their underlying policies and processes. However, the commercial secrecy surrounding algorithms again leaves society to speculate or express concern, without any means to examine platform policies and hold companies accountable for inadequacy or negligence.

With the recognition of the right to know algorithms, democratic participation, public safety, and social equality are the public interests undergirding the mandatory disclosure of the trade secrets of social media algorithms. This approach to recognizing a new legal right comports with the judiciary's past practice in handling trade secrets and the public interest. Courts have considered public policy considerations that justify disclosure, even at the expense of a trade secret developer's commercial interests. Most notably, in the case of *O'Grady v. Superior Court*,[248] the court rejected Apple Computer, Inc.'s categorical claim that there was not and could not be a public interest in its commercial trade secrets, providing examples of where free speech interests might prevail.[249] For instance, the court noted that secret business practices affect not only commercial welfare, "but the welfare of a whole industry, sector, or community," and timely disclosure "might avert the infliction of unmeasured harm on many thousands of individuals."[250] However, what is in the public interest or newsworthy is not limited to matters of safety. The court noted the "deeply rooted" nature of the constitutional right to acquire and share information, and discouraged courts from declaring what is and is not newsworthy.[251] Relevantly for social media algorithms, the court also noted that the increasing and unpredictable importance of technological developments to individual and collective life made it particularly difficult to declare that a disclosure is not newsworthy.[252]

### C. *Enforcing Social Media Companies' Responsibilities*

Recognition of the right to know algorithms would also reframe the nature and scope of social media companies' responsibilities, thereby offering a new perspective in considering whether their algorithms could be disclosed

---

[247] Chander, *supra* note 11, at 1028-30 ("First, because much of societal discrimination is subconscious or unconscious, it is less likely to be encoded into automated algorithms than the human decisionmakers that the algorithms replace. . . Second, even for programmers or companies who intend to discriminate, the process of coding itself is likely to cause programmers to shy away from actually encoding the discrimination. Even absent compelled disclosure through litigation, there is the danger that a hard-coded discrimination will be revealed later. . . Third, even if corporations engage in other kinds of wrongdoing, that does not mean that they are likely to intentionally manipulate algorithms to invidiously discriminate.").

[248] 44 Cal. Rptr. 3d 72 (Ct. App. 2006).

[249] *Id.* at 112; Samuelson, *supra* note 229, at 809-10.

[250] O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 112 (Cal. Ct. App. 2006).

[251] *Id.* at 112-15.

[252] *Id.*

to an appropriate extent. Under the influential Hohfeldian analysis of rights protection,[253] a legal right has four basic elements: the privilege, the claim, the power, and the immunity.[254] As to the claim element, a legal right correlates to a duty corresponding to the realization of the right.[255] an employer has a duty to pay employees their salaries because employees have a claim that their employer should pay their salaries on time. Hence, every claim-right correlates to a duty in one or more duty-bearers.

Ostensibly, the right to know algorithms carries a claim for informing the public of sufficient information concerning social media algorithms. Applying the Hohfeldian analysis, this claim would translate into a duty to disclose such information by social media companies. Therefore, the right to know algorithms would prevent trade secret rights over algorithms from being considered only in light of social media companies' private interests. Instead, their trade secret rights are innately attached with the appropriate disclosure responsibility. Considered in this way, a private entity's trade secret rights would not necessarily outweigh the public's right to know. By recognizing the right to know algorithms, the legal framework surrounding social media companies would change, potentially striking a balance between protecting trade secrets and promoting transparency for the benefit of users and society as a whole.

The right to know algorithms would prompt a closer examination of the public service functions performed by social media companies, highlighting the public interest aspect of their algorithms' trade secrets. Social media companies differ from many other private entities (such as Coca-Cola) that primarily engage in private commercial transactions, making their trade secrets less susceptible to mandatory disclosure under the right to know principle. While social media platforms operate as private companies, they essentially perform a variety of public service functions.[256] For instance, they facilitate public participation in art, politics, and culture, organize public conversation and communication, and curate public opinion through individualized feeds.[257] They enable users to engage with various aspects of society and serve

---

[253] *See generally* J.M. Balkin, *The Hohfeldian Approach to Law and Semiotics*, 44 U. MIAMI L. REV. 1119 (1990); Joseph William Singer, *The Legal Rights Debate in Analytical Jurisprudence from Bentham to Hohfeld*, 1982 WIS. L. REV. 975 (1982); Thomas D. Perry, *A Paradigm of Philosophy: Hohfeld on Legal Rights*, 14 AM. PHIL. Q. 41 (1977).

[254] Wesley Newcomb Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 26 YALE L.J. 710, 716 (1917) ("The chief purpose of the following pages is, however, to discuss, directly and exhaustively, only the first of the four general classifications above outlined, i.e., rights (or claims), privileges, powers, and immunities in personam and rights (or claims), privileges, powers, and immunities in rem.").

[255] *Id*. at 718 ("A paucital right, or claim, (right in personal) is either a unique right residing in a person (or group of persons) and availing against a single person (or single group of persons); or else it is one of a few fundamentally similar, yet separate, rights availing respectively against a few definite persons.").

[256] SUu, *supra* note 20, at 133 (discussing the information disseminator role played by technology companies).

[257] Jack Balkin, *How to Regulate (and Not Regulate) Social Media*, 1 J. FREE SPEECH L. 71, 75 (2021).

as forums for public discourse, where users can express their ideas and opinions and discuss current events. The private curation of public discourse is not new, as the exercise of editorial judgement by media organizations long predates the rise of social media.[258]

Public service functions, when executed correctly, hold significant value as they contribute to the marketplace of ideas and support democratic self-governance and cultural participation. Ensuring these values cannot solely rely on the legal norm that prohibits state censorship; it also demands that social media platforms create and foster a public sphere.[259] For platforms to effectively play this role, they must be trustworthy and trusted by users. Without trust, the exercise of free speech can devolve into a chaotic "a rhetorical war of all against all," undermining the objectives of free expression.[260] Currently, the secrecy and inscrutability of algorithm-automated curation of online speech present one of the most significant challenges to trust in social media algorithms as guardians of the public sphere.

Recognizing the right to know algorithms would aim to balance the need for transparency with the protection of proprietary information, enabling users to have more confidence in the platforms they use. This increased trust could lead to more meaningful public discourse, better democratic participa- tion, and a healthier public sphere overall. The absolute protection of social media algorithms as trade secrets could indeed be contrary to public interest if it supersedes the need for transparency in online speech curation. Greater transparency could enable the external improvement or correction of the consequences of technology.[261] By revealing how algorithms work, experts can identify potential biases, flaws, or unintended consequences and suggest improvements. Greater transparency helps users understand how algorithms influence their online experience,[262] enabling them to make more informed choices. At the very least, it would empower users to reject unsatisfactory platforms.[263] When users are aware of recommendation policies, they can choose platforms that align with their values or preferences.

Across the political spectrum, there is a growing appetite for algorithm transparency to better inform the public and restore trust in social media plat-

---

[258] *Id.*

[259] *Id.* at 78.

[260] *Id.* at 79.

[261] Will Knight, *Elon Musk's Plan to Open Source the Twitter Algorithm Won't Solve Anything*, WIRED (Apr. 27, 2022), https://www.wired.com/story/twitter-open-algorithm-problem [https://perma.cc/P75W-YMKN].

[262] Kerem Gülen, *Open-Source Twitter: What Could Go Wrong?*, DATACOUOMY (May 6, 2022), https://dataconomy.com/2022/05/open-source-twitter-algorithm-pros-cons [https://perma.cc/GJU4-G42F].

[263] Rashi Shrivastava, *Mastodon Isn't A Replacement For Twitter—But It Has Rewards Of Its Own*, FORBES (Nov. 4, 2022), https://www.forbes.com/sites/rashishrivastava/2022/11/04/mastodon-isnt-a-replacement-for-twitterbut-it-has-rewards-of-its-own/?sh=68f2e7c3a6eb [https://perma.cc/L582-5K65].

forms.[264] Some argue that transparency alone may not be enough, as users need the expertise and tools to act on the information shared.[265] However, even if transparency does not provide complete individual empowerment, it can still contribute to a higher degree of public trust toward social media. Moreover, as the government begins to regulate Big Tech more closely, this intervention may help improve trust in the public services provided by these platforms. Balancing transparency with the protection of trade secrets is cru- cial for maintaining a healthy public sphere and ensuring users can engage in meaningful discourse and democratic participation.

## IV. PROTECTIUG THE RIGHT TO KUOW ALGORITHMS

Based upon the right to know algorithms, I put forward in this part a multi-stakeholder approach to filling the regulatory vacuum concerning social media algorithms in the United States. Following this new approach, a multi-stakeholder governance mechanism should be launched to engage Congress, the relevant administrative agencies, and courts to take appropriate actions to protect the right to know social media algorithms. I also discuss how the multi-stakeholder approach is advantageous to several other models of algorithmic regulation as well as how to resolve the potential First and Fifth Amendment legal challenges posed in opposition to this approach.

### A. *A Multi-Stakeholder Approach*

#### 1. Legislative Principles

Recognition of the right to know social media algorithms would give legislators a legal basis for enacting laws that mandate the disclosure of such algorithms. It is thus of crucial importance to usher in legal principles to guide the legislative protection of the right to know social media algorithms. In this section, I propose transparency, intelligibility, and accountability as the three legal principles for the effective legal regulation of social media algorithms.

##### a. *Transparency*

To safeguard the right to know, it is essential to implement a transparency principle that mandates social media companies to disclose pertinent information about their algorithms. Although algorithmic transparency has been introduced to address various social media sectors, such as digital journalism, [266] its nature and scope remain somewhat vague and debatable. For example,

---

[264] Cristiano Lima, *Is 7is Congress's Best Shot to Open up the 'Black Box' of Social Media?*, WASH. POST (May 4, 2022), https://www.washingtonpost.com/politics/2022/05/04/is-this-congresss-best-shot-open-up-black-box-social-media [https://perma.cc/L9JU-F25H].

[265] Lillian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to Explanation' is Probably not the Remedy You are Looking for*, 16 DUKE L. & TECH. REV. 18, 67 (2017).

[266] *See* Nicholas Diakopoulos & Michael Koliska, *Algorithmic Transparency in the News Media*, 5 DIGITAL JOURUALISM 809, 813 (2017) ("The notion of algorithmic transparency in the news media is an attempt to articulate the mechanisms by which information about algorithms may be made public. Disclosing information about how algorithms drive various computational

Frank Pasquale proposes the concept of qualified transparency, which allows for varying degrees, types, and amounts of information to be disclosed to different actors depending on the specific purpose of each disclosure. [267] Margot Kaminski identifies two dimensions of algorithmic transparency: individualized transparency and systemic transparency. The former focuses on empowering individuals to contest automated decision-making processes controlled by algorithms by granting them access to the relevant information associated with these algorithms.[268] In contrast, systemic transparency seeks to reveal errors, biases, and discrimination present in both machine and human systems, enabling them to be addressed, mitigated, or even corrected.[269]

Despite its different conceptualization, the transparency principle is a necessary step in protecting the right to know, as it enables the appropriate disclosure of information about social media algorithms to the public or relevant authorities. Without such disclosure, neither the public nor authorities would have access to information about these algorithms, such as the types of news and advertisements recommended to users or the categories of personal data collected from them. Consequently, legislators should prioritize the adoption of transparency as a requirement for social media companies, laying the groundwork for administrative agencies and courts to evaluate the extent of algorithmic information disclosure. This can be achieved by weighing the public interests in attaining transparency against the trade secret values of the algorithms.

France has taken the initiative to introduce algorithmic transparency into its legislative regulation of social media platforms in order to combat election-related disinformation.[270] Enacted in 2018, the Manipulation of Information Law mandates social media platforms with over 5 million unique users per month to disclose information regarding their algorithms used for recommending, classifying, or referencing content related to debates of general interest.[271] To fulfill this requirement, platforms must publish two types of statistical information: (1) the proportion of direct access to content without reliance on recommendation algorithms; and (2) the proportion of indirect access attributable to either the platform's internal search engine algorithm or recommenda-

---

systems would allow users to determine the values, biases or ideologies in operation in order to understand underlying points of view of a news product.").

[267] *See* PASQUALE, THE BLACK BOX SOCIETY, *supra* note 5, at 140–188.

[268] Margot E. Kaminski, *Understanding Transparency in Algorithmic Accountability*, in THE CAMBRIDGE HAUDBOOK OF THE LAW OF ALGORITHMS 121, 129 (Woodrow Barfield ed., 2021) ("Individualized transparency consists of information flows targeted at the individual impacted by algorithmic decision-making.").

[269] *Id*. *See also*, Kung-Chung Liu, *Regulatory Issues of Data and Algorithms for the Data-Driven Economy*, 72 GRUR IUTERUATIOUAL 853, 859-861 (2023) (proposing that auditing algorithms as a means of promoting systemic transparency).

[270] Haochen Sun, *Regulating Algorithmic Disinformation*, 46 COLUM. J.L. & ARTS 367, 389-396 (2023).

[271] *Id*. at 392.

tion algorithm.[272] Furthermore, the law stipulates that platforms must make this information publicly available online in a free and open format.[273]

China has embraced algorithmic transparency as a broader legal requirement for social media platforms. Enacted in 2021, the Provisions on the Administration of Algorithm Recommendations for Internet Information Services[274] mandate that platforms inform users about the specific algorithmic services provided and appropriately publish "the basic principles, purposes, and main operating mechanisms of algorithmic recommendation services."[275]

Similarly, the proposed Artificial Intelligence (AI) Act[276] in the E.U. establishes transparency as a primary legal requirement for regulating the development and application of AI technology. Article 13 of the Act stipulates that "High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured..... "[277]

b. *Intelligibility*

Ensuring that information about algorithms is appropriately intelligible is another vital step in protecting the right to know. Merely granting citizens access to the information disclosed due to transparency requirements does not guarantee that they can comprehend it or gain insights into the operation of platforms. For example, the microblogging platform Mastodon has made Twitter's algorithm codes available on the software repository GitHub, enabling users to inspect these algorithms. However, this does not necessarily provide users with a clear understanding of Twitter's business structures and operations.[278] Therefore, it is essential to not only disclose algorithmic information but also present it in a manner that is easily comprehensible to users.

---

[272] *Id*. at 393.

[273] *Id*. at 393.

[274] Hualianwang Xinxi Fuwu Suanfa Tuijian Guanli Guiding [Provisions on the Administration of Algorithm Recommendations for Internet Information Services] (adopted at the 20th office meeting of the State Internet Information Office Nov. 16, 2021, effective Mar. 1, 2022) [hereinafter *Recommendation Algorithm Provisions*].

[275] *Id*.

[276] Proposal for a Regulation of The European Parliament and of the Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 [https://perma.cc/RA3V-4255].

[277] *Id*. at art.13.

[278] Chris Stokel-Walker, *The Problem With Elon Musk's Plan to Open-Source the Twitter Algorithm*, MIT TECH. REV. (Apr. 27, 2022), https://www.technologyreview.com/2022/04/27/1051472/the-problems-with-elon-musks-plan-to-open-source-the-twitter-algorithm/ [https://perma.cc/4Z8B-MWLS] ("But seeing the code behind an algorithm doesn't necessarily tell you how it works, and it certainly doesn't give the average person much insight into the business structures and processes that go into its creation."). *See also* Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 639 (2017) ("Most individuals are ill-equipped to review how computerized decisions are made, even if those decisions are reached transparently.").

Although algorithmic intelligibility and algorithmic explainability are often used interchangeably, some scholars differentiate between the two. Algorithmic explainability focuses on the need to clarify the processes or outputs of automated decision-making, while intelligibility has a narrower scope.[279] According to Zsolt Ződi, explainability involves "a clear and understandable connection . . . between the rules on the input side and . . . the decision on the output side." [280] In contrast, intelligibility refers to "presenting the whole thing in a linguistically understandable form." [281] While it might be possible to provide a comprehensive explanation of a machine-made decision for experts, the explanation may still be unintelligible for lay users who are affected by the decision-making process. As a result, it is essential to consider both explainability and intelligibility when disclosing algorithmic information to ensure that all users, regardless of their expertise, can understand the processes and outcomes of automated decision-making.

Some scholars adopt a broader definition of intelligibility, viewing it as a concept that encompasses "a collection of properties (including explainable, interpretable, and understandable) that all focus on what people can know or infer about a system."[282] These scholars argue that intelligibility conveys different meanings depending on the audience and identify three distinct types of intelligibility for affected people, users, and engineers. Affected people are those who do not directly interact with the system but are influenced by machine-made decisions, whereas users are individuals who actively participate in the system. Engineers, on the other hand, are the professionals responsible for designing, developing, and maintaining the system. By considering these different types of intelligibility, it is possible to better address the varying needs and levels of understanding among different stakeholders and ensure that the information about algorithms is accessible and comprehensible to all parties involved.

To protect the right to know, legislators should indeed require social media platforms to make the information about their algorithms appropriately intelligible, regardless of the varying degrees of intelligibility. Legislators can set the intelligibility principle in motion first by specifying what and how social media companies should provide explanations about their algorithms. For instance, they can propose that companies offer plain language explanations detailing the methods they use to recommend content to users and the ways they utilize users' personal data for commercial activities. Such plain language explanations can help make complex algorithms more accessible and understandable to a wider audience. However, the extent to which the intelligibility principle is to be achieved can be determined by relevant administra-

---

[279] Zsolt Ződi, *Algorithmic Explainability and Legal Reasoning*, 10 THEORY AUD PRACTICE OF LEGISLATIOu, 67, 76-77 (2022).

[280] *Id.* at 80.

[281] *Id.*

[282] Yishan Zhou & David Danks, *Di$erent "Intelligibility" for Di$erent Folks*, AIES '20: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 194, 194 (2020).

tive agencies and courts through appropriate procedures.[283] This approach allows for flexibility and adaptability in implementing intelligibility requirements while ensuring that users' right to know is respected and safeguarded.

The implementation of laws such as France's Manipulation of Information Law and China's Recommendation Algorithm Provisions demonstrates the growing recognition of the need for algorithmic intelligibility in social media companies. These laws require social media platforms to provide explanations about various aspects of their algorithms, ensuring that users can better understand the processes behind automated decision-making. While implementing the Manipulation of Information Law, the French government has required that the social media companies subject to this law should provide explanations about "elements relating to the purpose of the processing for which the algorithms have been programmed . . . rules defining this processing, the main characteristics of their implementation, the data processed and their sources, the processing parameters and their weighting.[284] China's Recommendation Algorithm Provisions explicitly require social media companies to publish and explain "the basic principles, purposes, and main operating mechanisms of algorithmic recommendation services in an appropriate manner."[285]

c. *Accountability*

Algorithmic accountability is another crucial legal principle that legislators should adopt to protect the right to know. This principle primarily addresses who should be held accountable for making social media algorithms transparent (legal subjects of accountability) and intelligible, and the legal consequences if those who are accountable fail to take the necessary actions (legal consequences of accountability).

Regarding the legal subjects of accountability, France's Manipulation of Information Law targets social media platforms with over 5 million unique users per month, requiring them to publish information about their algorithms used for specific purposes. [286] By focusing on platforms with a large user base, the law aims to ensure transparency and intelligibility for a significant portion of the population. China's Recommendation Algorithm Provisions, on the other hand, apply to providers of algorithmic recommendation services. [287] This broader scope covers not only social media platforms but also other services that utilize recommendation algorithms.

These examples illustrate the importance of identifying the legal subjects of accountability when implementing algorithmic accountability policies. By

---

[283] Katherine J. Strandburg, *Rulemaking and Inscrutable Automated Decision Tools*, 119 COLUM. L. REV. 1851, 1880 (2019) (arguing that "the choice to employ a machine-learning-based decision tool to evaluate particular decision criteria is fully explainable and has significant normative and policy implications that should be open to scrutiny").

[284] Sun, *supra* note 270, at 411 n.250.

[285] *Recommendation Algorithm Provisions*, *supra* note 274, at art. 16.

[286] Sun, *supra* note 270, at 392.

[287] *Recommendation Algorithm Provisions*, *supra* note 274, at arts. 6-15.

specifying who is responsible for ensuring algorithm transparency and intelligibility, legislators can effectively enforce these requirements and protect users' right to know.

In my opinion, potential legislation should initially target larger social media companies, as they are more likely to possess the necessary financial resources to handle compliance measures and serve as a more suitable testing ground for information disclosure exercises. Such legislation could require social media companies with over 30 million users in the United States, accounting for approximately 10% of the U.S. population, to participate in disclosure exercises. This benchmark would encompass the most popular social networking platforms in the United States, including Facebook, Instagram, TikTok, Twitter, Pinterest, LinkedIn, and Reddit, [288] as well as some smaller platforms like Nextdoor[289] and video-sharing and messaging planforms such as YouTube and WhatsApp.[290]

By focusing on these major platforms, the legislation can have a significant impact on the overall digital landscape in the United States, protecting users' right to know and promoting algorithmic transparency and intelligibility. Furthermore, if successful, the lessons learned from these initial disclosure exercises could then be applied to smaller platforms and other digital services that utilize algorithms, ultimately fostering a more responsible and transparent digital environment for all users.

As for the legal consequences of accountability, potential measures could include fines, penalties, or even suspension of services for companies that fail to comply with the requirements. By imposing such consequences, governments can motivate social media platforms and other algorithmic service providers to prioritize transparency and intelligibility, ultimately fostering a more responsible digital environment.

### 2. Administrative Regulation

Similarly, protection of the right to know algorithms could empower government agencies to create an administrative mechanism for regulating social media algorithms. Such a mechanism, as I will demonstrate, could serve to promote transparency, intelligibility, and accountability through the dynamic engagement of social media users and experts and robust oversight by the relevant administrative agencies.

---

[288] *See US Social Media Statistics 2022*, THE GLOBAL STATS., https://www.theglobalstatistics.com/united-states-social-media-statistics [https://perma.cc/QPC2-XKTP].

[289] Nextdoor has about 38 million U.S. users in 2022. *See id.*

[290] *See id.* ("FB Messenger is the most popular Messenger App in the US with 187.70 million active users. Facebook-owned FB Messenger has 61.10% of the country's total internet users. The second most popular on the list is iMessage, an instant messaging service developed by Apple Inc., with 40.20% penetration. It has 123.49 million active users. The third is Snapchat (118.89 million), which is really popular among teenagers, has 38.70% users. Forth in the list of 2022 social media chat apps is WhatsApp with 28.60% penetration.").

As shown in Part II, the right to know empowers administrative agencies to locate and obtain information from private entities and then disclose it to the greatest extent possible to protect the public interest.[291] For example, FOIA and the related environmental protection-related disclosure laws provide citizens with access to a wealth of environmental information held by private parties that agencies gather in carrying out their statutory functions and obligations. The Environmental Protection Agency (EPA) has the au- thority to request information from private parties, and, if those requests are not honored, enforcement mechanisms are available.[292] For example, section 114 of the Clean Air Act grants the EPA the authority to require regulated entities to maintain records, make reports, and "provide such other informa- tion as the Administrator may reasonably require" to fulfill its statutory obli- gations. The EPA also has the authority to enter the premises of regulated entities to gather information from existing records and is required to disclose that information should an individual file a FOIA request.[293]

The right to know social media algorithms would similarly allow the legislature to delegate legal power to regulate social medial algorithms. As proposed in the preceding section, Congress should enact new laws to protect this right based on three legal standards, namely, transparency, intelligibility, and accountability. It can then designate an administrative agency with the requisite expertise to enforce those standards in practice.

With such delegation of power, an administrative agency could protect the right to know social media algorithms by taking spontaneous actions to regulate social media algorithms. The Federal Communications Commission (FCC) is an administrative agency that regulates radio, television, wire, satellite, and cable communications across the U.S.[294] As the primary authority in U.S. communications law, the FCC has the power to "[r]evis[e] media regulations so that new technologies flourish alongside diversity and localism" and to "[d]evelop[] and implement[] regulatory programs."[295] It maintains jurisdiction over broadband access, fair competition, radio frequency use, *media responsibility*, *public safety*, and homeland security.[296] Therefore, the FCC can be designated as the administrative agency with the regulatory power to protect public interests pertaining to the right to know through focusing on media responsibility and public safety. Subsequently, the FCC may take proactive

---

[291] *See infra* Part II.A.

[292] Shannon M. Roesler, *The Nature of the Environmental Right to Know*, 39 ECOLOGY L.Q. 989, 1014 (2012).

[293] *Id.*

[294] *The FCC's Mission*, FED. COMMC'US COMM'U, https://www.fcc.gov/about/overview [https://perma.cc/SJF9-v94S].

[295] *What We Do*, FED. COMMC'US COMM'U, https://www.fcc.gov/about-fcc/what-we-do [https://perma.cc/9HQW-FH65].

[296] Federal Communications Commission, *2008 Performance and Accountability Report* (September 2008).

actions to minimize the dissemination of information that is harmful to democratic governance, public safety and social equality.

I suggest that the FCC should create an administrative mechanism to protect the right to know social media algorithms so as to implement the transparency, intelligibility, and accountability principles.[297] To develop the requisite regulatory expertise, the FCC could engage panels of social media experts and users to review the transparency and intelligibility of the algorithms involved in such social media company activities as content moderation, targeted advertising, and personal data collection. It could conduct the review process every two years and require major social media companies to submit reports on their algorithms for bi-annual review. Social media companies subject to the review would need to prepare materials about the algorithms they apply in relation to disinformation, submit them to the FCC ahead of the review period, and send officials to participate in the review pro- cess. The review panel could host cross-examining sessions, giving officials the opportunity to clarify various aspects of their companies' algorithms. After each review exercise, the panel would make recommendations on how the company should improve or rectify its algorithms, and the FCC could impose penalties on companies that fail to meet the review requirements or follow the panel's recommendations.

3. Judicial Protection

The judiciary is another institution that should be empowered to protect the right to know social media algorithms. Compared with the right to explanation, the right to know would put U.S. courts in a better position to protect public interests associated with social media algorithms. Under the European Union's General Data Protection Regulation (GDPR),[298] several data protection provisions mandate that E.U. citizens should be entitled to decide whether they can be subjected to algorithmically-controlled automatic deci- sion-making processes.[299] With these provisions, scholars argue that the GDPR protects a right to explanation, empowering E.U. citizens to demand that technology companies collecting their data disclose information about

---

[297] For a full account of this administrative mechanism, see Sun, *supra* note 270, at 408-16.

[298] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[299] Article 22.3 of the GDPR states:

> "In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."

their algorithms to them.[300] Hence, it has been suggested that the right should be applied to address algorithmic secrecy in the United States too.[301]

While reliance on the right to explanation opens new avenues of mitigating algorithmic secrecy, the right to know social media algorithms presents a more straightforward solution that eliminates the uncertainty surrounding the existence of a right to explanation under the GDPR.[302] Furthermore, it addresses whether such a right could be directly applied in countries like the United States. By relying on the long-established and protected right to know in the U.S., the policy considerations supporting this right can be used to justify expanding its scope to cover the transparency and intelligibility of social media algorithms.[303] In terms of policy, it would be more straightforward to introduce the right to know social media algorithms in the U.S. legal system, paving the way for U.S. courts to recognize and protect this right. As this article has demonstrated, the policy considerations undergirding the right to know can justify the expansion of this right to govern the transparency and intelligibility of social media algorithms. Meanwhile, the right to know social media algorithms offers broader legal protection of public interests compared to the right to explanation, which focuses solely on personal data protection.[304] The right to know social media algorithms not only safeguards personal data but also promotes transparency in addressing issues such as fake news and copyrighted materials handled by content moderation algorithms.

Courts can exercise their judicial review power to protect the right to know social media algorithms in the following two ways. First, courts could protect the public interest in algorithmic transparency through hearing law-

---

[300] *See* Andrew D. Selbst & Julia Powles, *Meaningful Information and the Right to Explanation*, 7 IUT'L DATA PRIVACY L. 233, 233 (2017) ("Automated decisions without any human intervention or understanding would seem to flout European ideas of autonomy and personhood."); Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L.J. 190, 209-17 (2019).

[301] *See* The White House, *Blueprint for an AI Bill of Rights*, https://www.whitehouse.gov/ostp/ai-bill-of-rights/ [https://perma.cc/NG5G-GEYU] ("You should know that an automated system is being used and understand how and why it contributes to outcomes that impact you."); Margot E. Kaminski &. Jennifer M. Urban, *The Right to Contest AI*, 121 COLUM. L. REV. 7, 1957, 1973, 2003 (2021) ("One tool for addressing bad AI decisions, gaining traction in some parts of the world but largely ignored in the United States, is contestation: giving individuals affected by AI decisions the right to challenge those decisions. Contestation without an explanation, in other words, is largely meaningless.").

[302] *See* Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 IUT'L DATA PRIVACY L. 76, 79 (2017); Sandra Wachter et al., *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, 31 HARV. J.L. & TECH. 841, 842 (2018); Byran Casey et al., *Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise*, 34 BERKELEY TECH. L.J. 143, 158 (2019) ("Despite the GDPR's concerted efforts to detail the protections enshrined under Articles 13, 14, 15, and 22, much uncertainty continues to shroud the Regulation's so-called 'right to explanation.'").

[303] *See infra* Part II.B.

[304] *See* Sylvia Lu, *Data Privacy, Human Rights, and Algorithmic Opacity*, 110 CAL. L. REV. 2087, 2113 (2022) ("Although Article 22 of the GDPR protects individuals against unjust automated decisions, it does not apply to corporate algorithmic decisions in a variety of contexts. ).

suits initiated by users of a social media platform against the FCC's review decisions. With the right to know algorithms, users can bring a lawsuit if they are not satisfied with an FCC's decision. They can request the court to review whether the FCC correctly made the decision on the transparency and intelligibility of the algorithmic information disclosed by the social media company concerned. An individual user is not allowed to launch a lawsuit of this type for himself or herself. Rather, users can only initiate class-action lawsuits because the right to know social media algorithms protects public interests such as democratic participation and social equality instead of individual interests. Hence, users should bring a class-action lawsuit on behalf of a group of users or all users of that platform. Another purpose of this arrangement is to shield social media companies from excessive litigation.

Second, courts could review whether social media companies have fulfilled their legal responsibilities in meeting the disclosure requirements for protecting the right to know algorithms. In these cases, social media companies could petition to courts to conduct judicial review of whether the FCC made a correct decision on whether it has fulfilled its disclosure responsibilities. Such a judicial review mechanism is intended to safeguard social media companies' legitimate interests in protecting their algorithms as trade secrets or their responsibilities in protecting their users' personal data.

As discussed earlier in this part, social media companies are not required to fully disclose all confidential information concerning their algorithms (e.g. a complete set of source codes of the algorithms).[305] Instead, they are obligated to make proportionate disclosure of such information so as to meet the transparency and intelligibility requirements.[306] Meanwhile, each social media company also has legal responsibilities to protect their users' personal data from being disclosed with the confidential information pertaining to their algorithms. Given that datasets are always intertwined with the development and application of algorithms, personal data might be disclosed together with the confidential information concerning such algorithms without authorization from users. Therefore, social media companies must either prevent such unauthorized disclosure of personal data or take technical measures such as encryption in order to preserve the anonymity of such data. They can thus request courts to review the legality of any administrative decisions requiring them to disclose their users' personal data in ways that would cause them to

---

[305] Katarina Foss-Solbrekk, *Three Routes To Protecting AI Systems and Their Algorithms Under IP Law: The Good, The Bad and The Ugly* (Mar. 2021), https://academic.oup.com/jiplp/article/16/3/247/6143561 [https://perma.cc/ME9U-XB2G] ("The algorithm is not shielded from the public for convenience. It is hidden to preserve trade secret status as this only remains intact for as long as the information remains confidential, meaning actors must take steps to ensure confidentiality and that there is little incentive nor reason for firms to reveal algorithmic information.").

[306] Laura Edelson, *Platform Transparency Legislation: The Whos, Whats and Hows*, Apr. 29, 2022, https://www.lawfareblog.com/platform-transparency-legislation-whos-whats-and-hows [https://perma.cc/UB7D-LZ2Y] (arguing that "limiting transparency to vetted researchers appears to be a mechanism to allow some limited sharing to vetted parties of potentially sensitive data that simply wouldn't be releasable to a public audience").

violate privacy law. These safeguards protect social media companies' commercial interests, ensuring that they are required to make proportionate (instead of full) disclosure of their algorithms only.

### B. *Advantages and Challenges*

#### 1. Advantages of the Multi-Stakeholder Approach

##### a. *Open-Source Model*

Making algorithms open source, according to some commentators, could address the problems with algorithmic secrecy.[307] Since Elon Musk's purchase of Twitter, considerable attention has been paid to the value of transparency with respect to recommendation algorithms. In response to Musk's suggestion that Twitter's algorithms be made open source, commentators have noted that greater transparency has the potential to educate users about the vast power and influence that platforms have over the content we consume.[308] Some have also highlighted the potential for transparency obligations to hold platforms accountable. If social media platforms were required to release their algorithms as open-source information, then their alleged political preferences and biases would be revealed to the public.[309] Furthermore, it has also been claimed that the open-source model of transparency would allow people unconnected to the platform to improve upon platforms' algorithms and make recommendations to platform developers.[310]

Although the open-source model ensures algorithmic transparency, it does not necessarily address the issues of algorithmic intelligibility and accountability. The mere publication of social media companies' algorithms does not automatically result in intelligibility. Companies must act in good faith to explain how they operate their algorithms and the user data and preferences involved.[311] Similarly, the open-source model does not settle the matter of whether social media companies should be held liable for the spread of harmful content on their platforms. Rather, companies could invoke the open-source model as an excuse to evade their responsibility to curb disinformation

---

[307] *See* Edward Lempinen, *Thwarting Disinformation, Defending Democracy—Scholar Sees A New Approach*, Feb. 14, 2022, https://phys.org/news/2022-02-thwarting-disinformation-defending-democracyscholar-approach.html [https://perma.cc/9REB-3ZBR] ("In an analysis published today (Feb. 11) in the journal *Science*, Nonnecke and co-author Camille Carlton detail the political measures that would force Facebook and other platforms to open access onto the oceans of data they collect from billions of users.").

[308] Kerem Gülen, *Open-Source Twitter: What Could Go Wrong?*, DATACONOMY (May 6, 2022), https://dataconomy.com/2022/05/open-source-twitter-algorithm-pros-cons/ [https://perma.cc/BQ45-G7QG].

[309] Will Knight, *Elon Musk's Plan to Open Source the Twitter Algorithm Won't Solve Anything*, WIRED (Apr. 27, 2022), https://www.wired.com/story/twitter-open-algorithm-problem/ [https://perma.cc/8582-47JS].

[310] Maxwell Adler, *Why Elon Musk Wants to 'Open Source' Twitter's Algorithms*, BLOOMBERG (Apr. 29, 2022), https://www.bloomberg.com/news/articles/2022-04-28/why-musk-wants-to-open-source-twitter-s-algorithms-quicktake [https://perma.cc/2BCS-Kv9L].

[311] *Id.*

by alleging that they have fulfilled the responsibility to release their algorithms for public scrutiny.

Compared with the open-source model, the multi-stakeholder approach has the advantage of establishing legal rules requiring social media companies to facilitate a better understanding of their algorithms among their users. Furthermore, the multi-stakeholder approach would require those companies to assume stronger legal responsibility to effectively curb social harms by altering the technical design of their algorithms.

b. *Public Trustee Model*

The public trustee model is another approach that has been proposed to tackle the social harms caused by social media algorithms. Drawing on previous proposals concerning social media platforms' fiduciary duties[312] and public interest doctrine,[313] Napoli and Graf argue that social media platforms should be deemed public trustees of the user data they aggregate and, accordingly, that members of the public who contribute personal data to such aggregation should be the beneficiaries.[314] They then apply the public trustee model to justify social media companies' responsibility to police harmful content on their platforms:

> Transferring this model to the social media context means that those platforms with privileged access to sufficiently large aggregations of user data to be considered a public resource would enter into a similar *quid pro quo* relationship, involving adherence to a set of public interest obligations. These obligations could involve policing/filtering certain types of content and/or amplifying other types of content. The key point here is that, through treating aggregate user data as a public resource, such content-related public interest obligations would be premised on a rational basis that has proven capable of withstanding First Amendment scrutiny.[315]

Although this approach elucidates social media companies' responsibility in relation to the data they have collected, it does not address algorithmic

---

[312] Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1209 (2016) ("People and organizations that have fiduciary duties arising from the use and exchange of information are information fiduciaries whether or not they also do other things on the client's behalf, like manage an estate or perform legal or medical services."); Balkin, *Free Speech in the Algorithmic Society*, *supra* note 1, at 1162 ("Who are the new information fiduciaries in the digital age? They are organizations and enterprises who collect enormous amounts of information about their end-users.").

[313] Philip M. Napoli and Fabienne Graf, *Social Media Platforms as Public Trustees: An Approach To 7e Disinformation Problem*, *in* ARTIFICIAL IuTELLIGEuCE AuD THE MEDIA 94, 108 (Taina Pihlajarinne and Anette Alén-Savikko eds., 2022)

[314] *Id.* at 109 ("In the framework being proposed here, user data aggregators such as Facebook and Twitter are the trustees. The public whose personal data are being aggregated and monetized are the beneficiaries. The trust property, in this case, is the aggregate user data.").

[315] *Id.* at 115.

transparency and intelligibility as the central problems with the legal regulation of algorithms in the digital age.[316] As Part II demonstrates, it is recommendation algorithms that unduly aggregate and share user data and amplify disinformation. Similarly, generative algorithms create and disseminate disinformation. Without subjecting such algorithms to the public property requirement that triggers the trustee-beneficiary relationship, the public trustee approach cannot bring forth new legal rules requiring social media companies to make their algorithms transparent and intelligible.

In contrast, multi-stakeholder approach deal less with the proprietary status of user data. Central to this approach are legal efforts to avert the black-box status of social media algorithms. Therefore, it calls for the establishment of an administrative review mechanism as a pilot program to impose legal responsibilities on social media companies to render their algorithms transparent and intelligible and to enforce those responsibilities.

### 2. Rising to the Potential Legal Challenges

#### a. *First Amendment-Based Challenges*

Social media companies might well launch legal challenges against the legislative and administrative regulation of their algorithms based on the First Amendment to the U.S. Constitution. The First Amendment guarantees freedom of speech by prohibiting Congress from making any law restricting the right of the press or individuals to speak freely.[317]

Under First Amendment jurisprudence, computer codes and search engine results produced by algorithms are likely to be protected as speech. Computer codes, by nature, are composed of programming languages. The purpose of codes is to facilitate communications between programmers and machines.[318] Unlike mute objects that can be used expressively, computer codes are "natural vessels for expression,"[319] conveying expressive meanings as do other forms of speech.[320] Even for those who do not consider codes to be

---

[316] Hilary Hurd, Note, *Fake News and the Looming "State Action" Problem*, HARV. J.L. & TECH. DIG. (2019), https://jolt.law.harvard.edu/digest/fake-news-and-the-looming-state-action-problem [https://perma.cc/P4DT-8S9X] ("While free speech advocates are right to demand that Facebook enhance transparency and accountability, treating Facebook as a state actor would exacerbate the fake news problem.").

[317] U.S. Const. amend. I.

[318] *See, e.g.,* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 449 (2d Cir. 2001); Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996).

[319] Tim Wu, *Machine Speech*, 161 U. PEuu. L. REV. 1495, 1500 (2013).

[320] *See* Junger v. Daley, 209 F.3d 481, 484–85 (6th Cir. 2000) ("Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment.") Kyle Langvardt, *Four Modes of Speech Protection for Algorithms*, *in* THE CAMBRIDGE HAuDBOOK OF THE LAW OF ALGORITHMS 543 (Woodrow Barfield ed. 2020) ("[Speech] protection might extend to the algorithm itself on the theory that the algorithm is speech. Insofar as computer code is a kind of language—and narrow it to source code if you like—then perhaps things that are written in code are 'speech,' just as this paragraph, written in English, is speech.").

speech, algorithms are not merely codes. Algorithms contain specific code-based commands from human programmers and are purposely delivered. Programmers communicate ideas and opinions concerning correlations among seemingly random datasets to machines and colleagues. Moreover, algorithmic outputs include search engine results, social media-targeted advertisements, rankings, and personalized recommendations.[321] Both courts and scholars have treated algorithmic outputs as protected speech. In a series of cases, Google has successfully defended its search results as protected speech deserving of constitutional protection,[322] and Amazon employed a similar strategy to protect Alexa voice recordings from police investigation.[323]

As a result, the multi-stakeholder approach's mandatory disclosure of social media algorithms could be subject to First Amendment scrutiny.[324] In my view, requiring the disclosure of specific information about social media algorithms would not violate the First Amendment.

The purpose of disclosing information under the right to know is not to alter how social media algorithms function or operate on their respective platforms. Such disclosure does not target the speech produced by the algorithms, that is, their generated outputs. Instead, this legal right necessitates the appropriate disclosure of how these algorithms work in relation to users on social media platforms, specifically focusing on the functioning of plat- form algorithms. Consequently, the disclosure requirement would not hinder social media platforms from utilizing algorithms. By maintaining the func- tioning of these algorithms, algorithmic transparency would not compromise free expression values.[325]

At the same time, Simultaneously, social media platforms have a responsibility to enable users to exercise their right to know about the algorithms used. As demonstrated, platforms should not solely operate based on their free speech claims; they must also accommodate measures that facilitate users' understanding of social media algorithms and improve their public services to better serve users' interests in algorithmic transparency and intelligibility.[326]

---

[321] Wu, *supra* note 319, at 1499.

[322] *See* Alan Sears, *Algorithmic Speech and Freedom of Expression*, 53 VAUD. J. TRAUSUAT'L L. 1327, 1339 (2021) ("In court, Google has repeatedly argued that its search results are protected speech and thus protected by the First Amendment.").

[323] *Id*. at 1340-41 ("Amazon argued that both the speech submitted to Alexa by the user, as well as the responses generated by Alexa, are protected by the First Amendment and thus subject to heightened scrutiny by a court.").

[324] Alan K. Chen, *Free Speech, Rational Deliberation, and Some Truths About Lies*, 62 WM. & MARY L. REV. 357, 421 (2020) ("To the extent that fake news does cause potentially broad social harms, but direct.censorship regulations are problematic under free speech law, policymakers could consider noncensorship alternatives to addressing such harms.").

[325] Max I. Fiest, *Why A Data Disclosure Law Is (Likely) Unconstitutional*, 43 COLUM. J. L. & ARTS 517, 529 (2020).

[326] *See supra* Part III.C. *See also*, Balkin, *Free Speech in the Algorithmic Society*, *supra* note 1, at 1209 ("From the standpoint of free speech values, the best solution would be for large international infrastructure owners and social media platforms to change their self-conception. Ideally, they would come to understand themselves as a new kind of media company, with obligations to

Therefore, an appropriate level of regulation for social media algorithms can be considered proportional to platforms' responsibility, as long as the regulation does not impose an excessively burdensome obligation on the platforms.

b. *Fifth Amendment-Based Challenges*

Another potential set of legal challenges might arise from the Fifth Amendment to the U.S. Constitution, which prohibits "private property [from] be[ing] taken for public use, without just compensation."[327] Social media companies may assert that their algorithms are private property because they are trade secrets. In *Ruckelshaus v. Monsanto Co.*,[328] the Supreme Court ruled that trade secrets constitute protected property under the Fifth Amendment. The mandatory disclosure of algorithms required by the right to know algorithms could therefore be considered a violation of the Fifth Amendment.

However, the Supreme Court has not categorically ruled out the disclosure of trade secrets based on public interest under the Fifth Amendment. In *Ruckelshaus*, the court examined the EPA's public disclosure of test data on pesticides under the *Berman v. Parker*[329] principle that government takings of property may be determined by Congress as long as they have a conceivable public character.[330] Exploring the background to relevant provisions of the Federal Insecticide, Fungicide, and Rodenticide Act, the court noted both the improvements in human productivity that pesticides had enabled and mounting public concern over their effects on human health and the environment.[331] Ultimately, it held that "public disclosure can provide an effective check on the decision-making processes of EPA and allows members of the public to determine the likelihood of individualized risks peculiar to their use of the product."[332]

At the same time, the disclosure of trade secrets required by the right to know social media algorithms does not constitute a *taking* of property per se under the Fifth Amendment. First, the proposed disclosure would not constitute the physical taking of social media algorithms. In *Loretto v. Teleprompter Manhattan CATV Corp*., the Supreme Court held that the permanent physical occupation of a private property by the government amounted to a taking, resulting in the need for just compensation to be paid to the rights owner.[333] However, the proportionate disclosure of trade secrets would not lead to the permanent possession of the information concerned because the rights owners would retain physical control of their algorithms and their application.

---

protect the global public good of a free Internet, and to preserve and extend the emerging global system of freedom of expression.").

327 U.S. Const. amend. V.

328 467 U.S. 986 (1984).

329 348 U.S. 26, 33 (1954).

330 *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1014-15 (1984).

331 *Id.* at 990.

332 *Id.* at 1016.

333 458 US 419 (1982).

Second, the proposed disclosure mechanism would not lead to the regulatory taking of social media algorithms. When it comes to the physical occupation of a property, a regulatory taking involves government regulation of the way the property is used, ultimately effectively deprived of all economically reasonable use or value of their property. In *Lucas v. South Carolina Coastal Council*, the Supreme Court ruled that a regulatory taking occurs when a governmental regulation deprives a property owner of all economically beneficial uses of his or her property.[334] The proposed mechanism for regulating social media algorithms, however, would not damage the algorithms' economic value because it would trigger only a proportionate disclosure. Consequently, the economic value of the algorithms powering social media platforms would be preserved.

## CONCLUSION

When President Johnson signed the FOIA into law back in 1966, he declared "a deep sense of pride that the United States is an open society in which the people's right to know is cherished and guarded."[335] However, this vision for a transparent American society has vanished. Ironically, the advent of social media and the digital age initially seemed to hold great promise for fostering transparency and open communication. Yet, the prevailing state of algorithmic secrecy on these platforms has led to an erosion of the very transparency that they were once expected to promote.

Many have lamented that our social media landscape is dominated by opaque algorithms unknown to citizens.[336] As I reveal in this article, while these algorithms are technically developed as black boxes, IP law legally reinforces their black box status by protecting them as trade secrets.

We must not allow such technical and legal arrangements to perpetuate a black box algorithmic society.[337] The right to know social media algorithms, as I propose in the article, aims to empower us to counter algorithmic secrecy. Legally, it entitles the public to demand a proportionate disclosure of trade secrets concerning social media algorithms. To safeguard the public interests undergirding this right, the government should initiate the proposed legal reforms to promote transparency and accountability in the algorithmic society. The implementation of the right to know in the realm of social media could serve as an essential starting point, setting the stage for new challenges and possibilities in addressing transparency across various AI sectors. By establishing a legal framework for social media algorithms, we create a founda-

---

[334] 505 U.S. 1003 (1992).

[335] Statement by the President Upon Signing the "Freedom of Information Act," 2 PUB. PAPERS 699 ( July 4, 1966).

[336] *See, e.g.,* PASQUALE, *supra* note 5, at 191 (2015) (arguing that the black box society is unjust because "[d]ata is becoming staggering in its breadth and depth, yet often the information most important to us is out of our reach, available only to insiders").

[337] *See, e.g.,* PHILIP M. NAPOLI, SOCIAL MEDIA AND THE PUBLIC INTEREST: MEDIA REGULATION IN THE DISINFORMATION AGE 188-93 (2019) (calling for legal and regulatory reforms aimed at curbing the algorithmic amplification of disinformation in the public interest).

tion that can be expanded to encompass other AI applications, such as those employed by government agencies, financial institutions, and generative AI systems. This legal foundation will not only enhance public understanding of algorithmic decision-making processes but also help refine the right to know as it adapts to the ever-evolving landscape of AI technologies. These dynamic developments, in turn, could lead to improved transparency and accountability, fostering trust and collaboration between the public and the entities harnessing the power of artificial intelligence.