Privacy and Disinformation

TIFFANY C. LI[†]

All three branches of the federal government have wrestled with how the law could or should regulate social media applications to mitigate the harms of disinformation. However, most proposed solutions make the same critical mistake: Lawmakers may focus on speech regulation or even economic regulation to solve for disinformation but these solutions do not actually address contemporary, technological vectors of disinformation. In today's increasingly technologically driven global speech environment, the lynchpin for disinformation is not speech but data.

In particular, algorithmic personalization is a new, technological factor that makes disinformation especially harmful. Luckily, data protection and privacy regulation can greatly curb the impact of algorithmic personalization and, correspondingly, disinformation harms as well. These privacy regulatory solutions also do not have the negative factors that make speech and economic regulatory solutions difficult and ineffective. Thus, lawmakers would be better off moving away from speech and economic regulation to instead focus on privacy regulation to mitigate the harms of disinformation, including disinformation found on foreign-owned social media applications, like TikTok.

Legal solutions that focus on data privacy, instead of pure speech regulation or economic regulation, are better solutions for disinformation for four reasons. First, privacy regulation addresses the root of the problem for today's disinformation: the technological factor of personalization, driven by technological developments like the internet and artificial intelligence ("AI"). Second, privacy regulations are more likely to pass constitutional muster, avoiding First Amendment roadblocks. Third, privacy regulations are likely less controversial to an American public primed to fear censorship. Finally, privacy regulations would be less likely to discriminate harshly against foreign companies, resolving international tensions around perceived economic protectionism and trade unfairness.

[†] Associate Professor of Law, University of San Francisco School of Law; Faculty Affiliate Fellow, Yale Law School Information Society Project. The author thanks Christina Spiesel and Laurin Weissinger for their support and feedback, as well as the editors of the UC Law Journal and the organizers of the "Chronically Online—Social Media Content Moderation's Struggle with the First Amendment" symposium.

TABLE OF CONTENTS

INTRODUCTION

Even a broken clock is right twice a day, but the U.S. government's mishandling of the TikTok situation has managed to be wrong more than twice already this year—and the year is not yet over. TikTok, the popular Chinese-owned[1] social media application, has generated controversy since it first appeared in the U.S. marketplace.[2] Some have accused the application of being a vector for Chinese propaganda, harmful disinformation, and very cheesy dance remixes.[3] But TikTok is not the only social media application accused of harboring or even supporting the spread of harmful disinformation. Similar allegations have been made for applications like Twitter[4], YouTube[5], and Facebook[6]—but, unlike TikTok, these three applications are owned by U.S. companies.

All three branches of the federal government have wrestled with how the law could or should regulate social media applications to mitigate the harms of disinformation. However, most proposed solutions make the same critical mistake: Lawmakers may focus on speech regulation or even economic regulation to solve for disinformation, but these solutions do not actually address contemporary, technological vectors of disinformation. Additionally, both speech and economic regulatory solutions come with a myriad of negative externalities that makes them untenable and unpopular, as will be discussed further in this paper.

In today's increasingly technologically driven global speech environment, the lynchpin for disinformation is not speech but data. In particular, algorithmic personalization is a new, technological factor that makes disinformation especially harmful. Luckily, data protection and privacy regulation can greatly curb the impact of algorithmic personalization and, correspondingly, disinformation harms as well. These privacy regulatory solutions also do not

---

1. Technically, the parent company ByteDance claims the U.S. subsidiary TikTok is independent, though this claim is controversial. *See* Laura He, *Wait, Is TikTok Really Chinese?*, CNN BUSINESS (Mar. 28, 2024, at 8:21 AM EDT), https://www.cnn.com/2024/03/18/tech/tiktok-bytedance-china-ownership-intl-hnk/index.html.

2. *See* David Hamilton, *How TikTok Grew from a Fun App for Teens into a Potential National Security Threat*, AP NEWS (Jan. 19, 2025, at 5:16 AM PDT), https://apnews.com/article/tiktok-timeline-ban-biden-india-d3219a32de913f8083612e71ecf1f428.

3. *See* Ken Dilanian, *TikTok Says It's Not Spreading Chinese Propaganda. The U.S. Says There's a Real Risk. What's the Truth?*, NBC NEWS (Sept. 16, 2024, at 3:00 AM PDT), https://www.nbcnews.com/investigations/tiktok-says-not-spreading-chinese-propaganda-us-says-real-risk-rcna171201.

4. *See, e.g.*, Miah Hammond-Errey, *Elon Musk's Twitter Is Becoming a Sewer of Disinformation*, FOREIGN POLICY (July 15, 2023, at 7:00 AM), https://foreignpolicy.com/2023/07/15/elon-musk-twitter-blue-checks-verification-disinformation-propaganda-russia-china-trust-safety.

5. *See, e.g.*, Dan Milmo, *YouTube Is Major Conduit of Fake News, Factcheckers Say*, GUARDIAN (Jan. 12, 2022, at 12:00 AM EST), https://www.theguardian.com/technology/2022/jan/12/youtube-is-major-conduit-of-fake-news-factcheckers-say.

6. *See, e.g.*, Yunkang Yang, Matthew Hindman & Trevor Davis, *Visual Misinformation Is Widespread on Facebook—and Often Undercounted by Researchers*, THE CONVERSATION (Jun. 30, 2023, at 8:37 AM EDT), https://theconversation.com/visual-misinformation-is-widespread-on-facebook-and-often-undercounted-by-researchers-202913.

have the negative factors that make speech and economic regulatory solutions difficult and ineffective. Thus, lawmakers would be better off moving away from speech and economic regulation to instead focus on privacy regulation to mitigate the harms of disinformation, including disinformation found on foreign-owned social media applications, like TikTok.

Legal solutions that focus on data privacy, instead of pure speech regulation or economic regulation, are better solutions for disinformation for four reasons. First, privacy regulation addresses the root of the problem for today's disinformation: the technological factor of personalization, driven by technological developments like the internet and artificial intelligence ("AI"). Second, privacy regulations are more likely to pass constitutional muster, avoiding First Amendment roadblocks. Third, privacy regulations are likely less controversial to an American public primed to fear censorship. Finally, privacy regulations would be less likely to discriminate harshly against foreign companies, resolving international tensions around perceived economic protectionism and trade unfairness.

This Article adds to the scholarly literature on social media, speech regulation, privacy regulation, and emerging technologies. Many scholars have written about legal issues involving disinformation,[7] and many others have written about legal issues involving data privacy.[8] Some have written (mostly in critique) about proposed speech regulations to solve disinformation,[9] and others have written about the connection between disinformation and privacy regulation.[10] However, there has not yet been a scholarly law review article that

7. *See, e.g.*, Nina I. Brown, *Deepfakes and the Weaponization of Disinformation*, 23 VA. J.L. & TECH. 1, 2 (2020); Audrey C. Normandin, *Redefining "Misinformation," "Disinformation," and "Fake News": Using Social Science Research to Form an Interdisciplinary Model of Online Limited Forums on Social Media Platforms*, 44 CAMPBELL L. REV. 289, 289 (2022); Enrique Armijo, *Lies, Counter-Lies, and Disinformation in the Marketplace of Ideas*, 100 IND. L.J. 193, 193 (2024); Jason Pielemeier, *Disentangling Disinformation: What Makes Regulating Disinformation So Difficult?*, 2020 UTAH L. REV. 917, 917–18; Fernando Nuñez, *Disinformation Legislation and Freedom of Expression*, 10 U.C. IRVINE L. REV. 783, 784–85 (2020).

8. There is a *very* small sample of the abundantly growing scholarly space that is privacy law. *See, e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 477–78 (2006); Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. & HIGH TECH. L. 357, 357 (2011); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1906 (2013); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1701 (2010); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1193–94 (1998); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1461 (2000); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1609 (1999); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1125 (2000).

9. *See, e.g.*, Wes Henricksen, *Disinformation and the First Amendment: Fraud on the Public*, 96 ST. JOHN'S L. REV. 543, 556 (2022); Ari B. Rubin, *Disinformation on Trial: Fighting Foreign Disinformation by Empowering the Victims*, 43 CARDOZO L. REV. 969, 973 (2022); Russell L. Weaver, *Remedies for "Disinformation"*, 55 U. PAC. L. REV 185, 203 (2024); Nuñez, *supra* note 7, at 792-97.

10. *See, e.g.*, Haochen Sun, *Regulating Algorithmic Disinformation*, 46 COLUM. J.L. & ARTS 367, 371 (2023); Wayne Unger, *How the Poor Data Privacy Regime Contributes to Misinformation Spread and Democratic Erosion*, 22 COLUM. SCI. & TECH. L. REV. 308, 310 (2021); Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1758 (2019).

puts all the pieces together to provide a comprehensive discussion of why speech and economic regulation fail and why privacy regulation can solve for disinformation in today's technologically driven speech environment. This Article contributes by first showing why technological developments have inextricably intertwined privacy and disinformation, and second explaining why privacy regulation is the best solution for today's disinformation, particularly where speech regulation and economic regulation fail.

This Article proceeds in four parts. First, the Article introduces the concept of disinformation and explains why lawmakers must solve the problem of disinformation. Second, it explains how the internet and AI have fueled a new era of disinformation, in which disinformation is increasingly personalized. Third, it explains why two proposed solutions—speech and economic regulation—do not solve for modern disinformation problems. Finally, it proposes privacy law as the best solution for disinformation as it exists today.

I. DISINFORMATION HARMS

This Part of the Article will explain the contemporary disinformation landscape, including arguments for why disinformation is harmful and why governments ought to attempt to mitigate those harms.

This Article defines disinformation as false information intentionally spread to cause harm. Disinformation is distinct from misinformation, which can be understood as false information that spreads without a concerted intention to deceive. Disinformation is also distinct from propaganda, though there is some overlap. Propaganda is "false or misleading information or ideas addressed to a mass audience by parties who thereby gain advantage, . . . created and disseminated systematically [in a manner that] does not invite critical analysis or response."[11] Thus, while some propaganda efforts can include disinformation, other propaganda efforts may include spreading true information. Additionally, while some disinformation is political in nature or comes from state actors, not all disinformation is technically tied to politics or state actors. Jason Pielemeier notes that it is often difficult to determine the boundaries of disinformation when compared to other categories of speech, particularly other categories of harmful speech, like terrorist incitement and hate speech.[12] This blurring of lines can mean that well-intentioned proposals that seek to regulate disinformation as speech run the risk of over-censorship and violate free speech and free expression rights.

11. Thomas Huckin, *Propaganda Defined*, *in* PROPAGANDA AND RHETORIC IN DEMOCRACY: HISTORY, THEORY, ANALYSIS 118, 126 (Gae Lyn Henderson & M. J. Braun eds., 2016) (emphasis omitted).

12. Pielemeier, *supra* note 7, at 922.

Disinformation is harmful for many reasons. Disinformation can spread false information related to health with serious consequences for public health.[13] Disinformation can cause political tensions and upset national elections.[14] Disinformation can threaten national security,[15] including through the aforementioned effects on public health and political processes. More fundamentally, disinformation threatens individual autonomy because disinformation campaigns seek to manipulate individuals and populations through false information.[16] Disinformation is also a critical threat to democracy because it warps democratic discourse and takes away citizens' rights to autonomously decide for themselves how to participate in the governing of their own people.[17]

Disinformation is a problem that both lawmakers and technology platforms must work to solve. It is, however, a difficult problem, particularly as it involves core American values of free speech and a free economy. On the other hand, Wes Henricksen argues that disinformation is harmful in so many different ways that any legal solutions must first take into account the immense harms that disinformation causes, which could outweigh any countervailing speech or other values.[18] The harms caused by disinformation are indeed immense. However, this Article will show how privacy law can solve for disinformation by attacking the personalization factor that other solutions ignore.

Having established the foundational concept of disinformation, as well as its harms, this Article will next provide a sociotechnical analysis of how disinformation actors spread their messages to individuals around the world, aided by new technologies like the internet and AI.

II. TECHNOLOGY'S IMPACT ON PRIVACY AND DISINFORMATION

This Part will explain how the internet and AI have, together, created the perfect conditions for personalized propaganda and disinformation. This Part will also show why personalization has become a critical factor in the spread of disinformation's harms, which will in turn provide the foundation for understanding why lawmakers ought to focus on regulations that attack the factor of personalization.

---

13. *See, e.g.*, Claudia E. Haupt & Mason Marks, *FTC Regulation of AI-Generated Medical Disinformation*, 332 JAMA 1975, 1975 (2024); Michael L. Rustad & Thomas H. Koenig, *Creating a Public Health Disinformation Exception to CDA Section 230*, 71 SYRACUSE L. REV. 1251, 1257 (2021).

14. *See, e.g.*, YOCHAI BENKLER, CASEY TILTON, BRUCE ETLING, HAL ROBERTS, JUSTIN CLARK, ROBERT FARIS, JONAS KAISER & CAROLYN SCHMITT, MAIL-IN VOTER FRAUD: ANATOMY OF A DISINFORMATION CAMPAIGN 7 (2020).

15. *See, e.g.*, Janis Sarts, *Disinformation as a Threat to National Security*, *in* DISINFORMATION AND FAKE NEWS 23, 31–32 (Shashi Jayakumar, Benjamin Ang & Nur Diyanah Anwar eds., 2021).

16. *See, e.g.*, Wes Henricksen, *The Price of Disinformation*, U.C. IRVINE L. REV. (forthcoming 2025) (manuscript at 40).

17. *See, e.g.*, Spencer McKay & Chris Tenove, *Disinformation as a Threat to Deliberative Democracy*, 74 POL. RSCH. Q. 703, 709 (2021).

18. Henricksen, *supra* note 16 (manuscript at 55).

A. THE INTERNET'S IMPACT ON DISINFORMATION

The greatest transformation in our modern information society is the advent of the internet. Certainly, one day (perhaps sooner than we think), a statement like the preceding will read as outdated and naïve.[19] However, today, there is no technology with greater impact on the spread of information, communication, and discourse than the internet.[20] The internet, a network of networks, connects individuals and organizations both locally and across the globe, through instantaneous[21] access.[22] The internet has accelerated and amplified the reach of communications while also democratizing both access to and participation in local and global discourse.[23] However, these benefits have also come with a slew of risks and harms—including new forms of disinformation, propaganda, and other harmful speech.[24]

Disinformation is not a new phenomenon; however, the way that disinformation actors create and spread disinformation has changed, as the media of communications have changed. The way that individuals receive and perceive disinformation has also changed, as this Article will explain. Many of these changes may be due to the rise of the internet. Yale Law School Professor Jack Balkin reminds us that it is not only the novelty of new technologies that merits study, but also what those new technologies reflect about changes in society.[25] As the internet has developed, individuals have become accustomed to instantaneously accessing information from all over the world, at all times of day. Individuals also expect to be able to communicate openly through a variety of different platforms that host user-generated content, and they expect that their communications will be accessible by others. Ultimately, the internet has flattened the traditional media landscape, as individuals do not have to rely on a few traditional media outlets for information but instead have nearly endless sources of media and information to consume. Additionally, every individual has a chance of having their communications read or heard by anyone in the world, which democratizes both access to information and speech.

---

19. Many legal scholars have written on the impact of the internet on communication and discourse, and corresponding impact on speech norms and related legal issues. *See, e.g.*, 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, 58 (2004); Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805, 1806 (1995); DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 57 (2014).

20. KEATS, *supra* note 19.

21. Or nearly so.

22. Except where access is blocked, by the actions of governments or otherwise.

23. *See, e.g.*, REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM 6 (2012).

24. *See, e.g.*, CITRON, *supra* note 19; Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, 91 B.U. L. REV. 1435, 1458 (2011); Mary Anne Franks, *Redefining "Revenge Porn" Reform: A View from the Front Lines*, 69 FLA. L. REV. 1251, 1308–23 (2017).

25. Balkin, *supra* note 19, at 2.

Before the internet, the information landscape was arguably dominated by large media companies who controlled the newspapers, radio stations, and television stations. Today, the information landscape is increasingly controlled by large technology corporations, especially those that own or operate platforms that host user-generated content. These technology corporations include Facebook, Google, X (formerly known as Twitter), and today, ByteDance (owner of TikTok). These "Big Tech" companies control a large share of the information marketplace—a consolidation of power some scholars find worrisome.[26] Annemarie Bridy and Frank Pasquale have argued that large technology corporations today function almost as sovereign nations.[27]

Today, large technology corporations in the internet space act as what Professor Kate Klonick has called "new governors," assuming the roles previously held by state governors in regulating speech.[28] Professor Balkin argues that our contemporary speech environment exhibits a pluralist model of speech regulation. In describing today's triangular online speech environment, he states that speech is regulated by three parties: state and supra-national entities, companies that operate digital infrastructure, and speakers who use digital infrastructure to communicate.[29] Whatever the model, it is clear that state actors are no longer the only regulators of individual or organizational speech. Of course, media and telecommunications always played a regulatory role in information and communications. However, the increased access to direct communications platforms has shifted the balance of power in speech regulation. Technology corporations now are arguably the most powerful regulators of speech.

Perhaps it is too obvious to note that governments do not traditionally enjoy it when private actors attempt to take powers traditionally held by the state. Today, technology corporations arguably have taken over the role and the responsibility of regulating speech online. But governments still play a strong role in regulating speech, even if it is indirectly, through regulation of those technology corporations as this Article will explain. Disinformation is one of those harmful speech problems that both governments and technology corporations must work together to solve. Understanding the new information environment is key to successfully solving the problem.

---

26. *See, e.g.*, JULIE E. COHEN, BETWEEN TRUTH AND POWER 99–100 (2019); Nikolas Guggenberger, *Moderating Monopolies*, 38 BERKELEY TECH. L.J. 119, 127 (2023); Lina M. Khan, *The Separation of Platforms and Commerce*, 119 COLUM. L. REV. 973, 983–84 (2019).

27. Annemarie Bridy, *Remediating Social Media: A Layer-Conscious Approach*, 24 B.U. J. SCI. & TECH. L. 193, 195 (2018); Frank Pasquale, *From Territorial to Functional Sovereignty: The Case of Amazon*, LAW & POL. ECON. PROJECT BLOG (Dec. 6, 2017), https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/.

28. Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1603 (2018).

29. 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, 1187–88 (2018).

Part II demonstrated how the rise of the internet changed the modern speech landscape, and with it, the problem of disinformation. However, the internet alone is not to blame for modern disinformation.

B. AI'S IMPACT ON DISINFORMATION

Another technological change that has influenced the development of the modern disinformation landscape is AI—specifically algorithmic personalization and recommendation mechanisms.

While the field of AI is rapidly evolving, a few baseline definitions can be helpful for a legal discussion.[30] AI refers to "any form of intelligence that is man-made or artificial, generally relating to the idea of a constructed machine intelligence that could potentially equal the intelligence of a human being."[31] There are many forms of AI that can be used for content creation, moderation, and targeting. One such form of AI is machine learning. Machine learning refers to a form of AI in which a computer draws conclusions or makes predictions based on data that is fed into a machine learning model, an algorithm trained on initial datasets.[32]

Two types of AI applications are particularly relevant to our discussion of disinformation on the internet: generative AI applications and algorithmic recommendations. Generative AI refers to applications that allow users to input a prompt (set of instructions) for a computer to generate a desired response that usually consists of content (text, image, audio, or video). Algorithmic recommendations refer to recommendations made to individuals, not manually, but through machine learning algorithms.

University of Hong Kong Faculty of Law Professor Haochen Sun argues that, today, the use of AI (particularly generative AI and recommendation algorithms) has created a new phenomenon of "algorithmic disinformation."[33] Disinformation actors may be able to use AI to create disinformation content through generative AI applications. These actors could then also manipulate recommendation algorithms to target their disinformation content to specific audiences. Thus, like the internet, AI has changed the field of disinformation.

C. NEW PRIVACY RISKS AND INVASIONS

The internet has transformed our conceptions of privacy and expanded the scope of privacy risks and invasions. Digital privacy and data protection have emerged as paramount concerns for civil liberties and individual rights. The internet generates new privacy concerns including data tracking, where

30. Note that the following are high-level definitions that do not capture the full spectrum of AI or machine learning. Certainly, there are more forms of AI that exist and are being used today, even in speech contexts. But a lengthy discussion is out of scope for this article.

31. Tiffany C. Li, *Algorithmic Destruction*, 75 SMU L. REV. 479, 484 (2022).

32. *Id.* at 486.

33. Sun, *supra* note 10, at 373–74.

companies or individuals track user behavior across various websites and applications using cookies and other persistent identifiers. The harms of digital privacy invasions may be even worse when we factor in location data that allows bad actors to track individuals at every moment of the day, through their mobile devices or even their cars.[34] The internet has also created vectors for privacy invasions related to sensitive data, including financial data,[35] health data,[36] biometric data (data related to or coming from the body),[37] genetic data,[38] and children's data[39]. Websites and applications collect information on individuals to build user profiles for a more complete picture of a person's identity, habits, and even thoughts. The continual, expansive collection of data creates more privacy risks.[40] Data privacy harms compound as data is collected, shared, sold, and repackaged by data brokers.[41] Internet-related privacy harms are also unequal, disproportionately affecting already marginalized groups.[42]

The use of AI has also transformed the world of privacy.[43] This includes recommendation algorithms and generative AI. Professor Sun identifies three categories of recommendation algorithms: (1) collaborative filtering, which recommends content to users based on what similar users enjoy; (2) content-based filtering, which recommends content to users based on user behavior; and (3) hybrid systems, which use elements of both collaborative and content-based filtering.[44] It is possible that recommendation algorithms may incentivize technology corporations to collect a significant amount of user data, in an attempt to build more accurate recommendation algorithms. Generally, platforms have an incentive to keep users engaged with their websites and apps. Thus, platforms may wish to recommend content that users will continue to interact with. To do this, platforms may collect data on past user behavior, user

34. The Daily, *Your Car May Be Spying on You*, N.Y. TIMES (Mar. 18, 2024), https://www.nytimes.com/2024/03/18/podcasts/the-daily/car-gm-insurance-spying.html.

35. *See, e.g.*, Ana Granova & J.H.P. Eloff, *A Legal Overview of Phishing*, COMPUT. FRAUD & SEC., July 2005, at 6, 6.

36. *See, e.g.*, Tiffany Li, *Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis*, 52 LOY. U. CHI. L.J. 767, 773 (2021).

37. *See, e.g.*, Ramona Pringle, *Controversial Clearview AI App Could 'End Privacy.' So, What Now?*, CBC NEWS (Feb. 1, 2020, at 1:00 AM PST), https://www.cbc.ca/news/science/clearview-app-privacy-1.5447420.

38. *See, e.g.*, Mason Marks & Tiffany Li, *DNA Donors Must Demand Stronger Protection for Genetic Privacy*, STAT NEWS (May 30, 2018), https://www.statnews.com/2018/05/30/dna-donors-genetic-privacy-nih.

39. Stacey B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, 66 EMORY L.J. 839, 844 (2017).

40. The Supreme Court considered this issue in *U.S. v. Jones*, 565 U.S. 400 (2012), and again in *Carpenter v. U.S.*, 585 U.S. 296 (2018), forming what is called the "mosaic theory" of privacy. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 328 (2012).

41. Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. 595, 596 (2004).

42. Tiffany C. Li, *Privacy as/and Civil Rights*, 36 BERKELEY TECH. L.J. 1265, 1278–79 (2021).

43. Daniel J. Solove, *Artificial Intelligence and Privacy*, 77 FLA. L. REV. 1, 1–4 (2025).

44. Sun, *supra* note 10, at 374.

demographic data (which could include location data), and data of similar users. Thus, the cornerstone of recommendation algorithms is personal data.

The use of generative AI also changes privacy. For example, the development of large language models often may necessitate data privacy invasions. To develop generative AI applications, programmers (usually, but not always, at large technology corporations)[45] typically begin by amassing a large amount of data,[46] sometimes by scraping data from public and private websites.[47] For example, programmers may collect a large amount of text written by humans (or machines) to train generative AI applications that produce textual output. Or, for another example, programmers may also collect a large number of real photographs of human beings to train generative AI applications that produce images of human faces or bodies. Because many current generative AI models rely on large quantities of data, programmers may be incentivized to collect increasingly large quantities of data, which could include personal data. Thus, these applications increase the risks of privacy invasions and unauthorized collection and use of personal information, including sensitive biometric information (like photographs of faces).

D. THE NEW DISINFORMATION IS PERSONALIZED

The technological phenomena of the internet and AI have combined to create a critical vector for disinformation attacks: personalization. This Article argues that personalization is at the heart of the modern disinformation problem. Understanding how the rise of the internet and the use of AI have personalized disinformation is important to understand how regulatory solutions can solve this problem.

Today, disinformation is increasingly personalized. This personalization occurs in three ways. First, content is personalized: as the internet has flattened the media landscape and AI has made content generation cheaper, faster, and easier, disinformation actors can now create larger volumes of content,[48] allowing for content tailored to increasingly narrow audiences. Second, content is personally targeted: by using the personal data collected from internet applications, along with algorithmic recommendations, disinformation actors

45. Companies like OpenAI, Microsoft, and Google have raced to leadership in the generative AI field, but this field is rapidly changing.

46. This is not strictly necessary. For example, DeepSeek made headlines in 2025 for announcing that they had developed a way to train their generative AI models at low cost, partially due to a training process that builds on inferences made by other generative AI models, bypassing the need for expensive data collection. *See* Kevin Collier & Jasmine Cui, *OpenAI Says DeepSeek May Have 'Inappropriately' Used Its Data*, NBC NEWS (Jan. 30, 2025, at 7:09 AM PST), https://www.nbcnews.com/tech/tech-news/openai-says-deepseek-may-inapproriately-used-data-rcna189872. This led to accusations from other AI companies that DeepSeek had stolen their hard-earned data (or the fruits of it). *Id.*

47. Daniel J. Solove & Woodrow Hartzog, *The Great Scrape: The Clash Between Scraping and Privacy*, 113 CALIF. L. REV. (forthcoming 2025) (manuscript at 9).

48. Noémi Bontridder & Yves Poullet, *The Role of Artificial Intelligence in Disinformation*, DATA & POL'Y, Nov. 21, 2021, at 1, 3.

are able to effectively target tailored content, including to the most vulnerable individuals. Third, interactions with content are personal: disinformation actors are now able to use the direct communication access of social media applications, along with personal information gleaned from the internet, to personalize (and sometimes falsify) interactions with individuals.

1. Content Creation Is Personalized

Personalization has transformed disinformation content. New technologies have made disinformation content creation cheaper, faster, and easier, as this section will discuss. Generative AI applications allow disinformation perpetrators to quickly and easily create disinformation content, including text, audio, image, and video.[49] This can even include the creation and spread of deepfakes, inauthentic images, audio, or video that appears authentic to the untrained eye.[50] Bad actors can use tracking methods to collect information about an individual based on internet activity, revealing information that could help build a profile of each individual. These personal profiles can then make it simpler for disinformation actors to create disinformation content that is personalized for increasingly narrow segments of the population—hypothetically even specific individuals.[51] While it would be difficult to create personalized content at large scales manually, it could become much simpler, faster, and cheaper to do so through generative AI. Thus, the internet and AI have combined to fuel personalization of disinformation content, at scale.

2. Content Is Personally Targeted

Personalization has also transformed the targeting function of disinformation dissemination. The same tracking and profiling techniques that can aid in the creation of narrowly tailored, personalized disinformation content can also help disinformation actors reach their desired audiences. Disinformation actors can manipulate the recommendation algorithms on social media applications so that they ensure their tailored, personalized content reaches the desired audiences.[52] Social media applications can already recommend content to users based on past behavior, which could lead users to see more and more of the same kinds of content.[53] Thus, once disinformation

49. Sun, *supra* note 10, at 377–79.

50. Chesney & Citron, *supra* note 10.

51. *See* Bontridder & Poullet, *supra* note 48, at 5.

52. Sun, *supra* note 10, at 374–75.

53. *See, e.g.*, Megan A. Brown, James Bisbee, Angela Lai, Richard Bonneau, Jonathan Nagler & Joshua A. Tucker, *Echo Chambers, Rabbit Holes, and Algorithmic Bias: How YouTube Recommends Content to Real Users* 2– 4 (Nov. 11, 2022) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4114905.

actors are able to hook a user onto a certain kind of content, they may be able to further instill their false messages into the minds of individuals.[54]

3. Interactions are Personalized

Personalization has also transformed inauthentic social interactions used as part of disinformation campaigns. As previously discussed, disinformation actors can now use technological tools to increase interactions with target individuals. The internet has made it possible for individuals to easily communicate with each other, and easily post and access information—including disinformation. This new medium of online communication has increased abilities for bad actors to engage with, manipulate, and harm individuals. For example, extremist groups, like ISIS, use social media profiles to communicate with individuals—sometimes to radicalize them and convince them to participate in violent terrorist attacks.[55] The Supreme Court took on the cases of *Gonzalez v. Google* and *Twitter v. Taamneh* in 2023.[56] Both cases involved accusations that social media companies were aiding and abetting extremism and violent extremist attacks through hosting content created by extremist groups and allowing such content to reach individuals who would later participate in extremist attacks. These cases show how the rise of the internet has helped fuel personalized disinformation interactions.

Further, bad actors can more effectively interact with target individuals in a personal manner by gleaning personal information from targets' public and private social media accounts and using that information to build closer relationships. This can amplify the harmful effects of disinformation. New AI-powered applications can also help bad actors interact with target individuals by automating translations and generating responses and queries that mimic natural language. Generative AI applications can even help bad actors adopt false identities to manipulate individuals—something that has already accelerated cyber fraud and scams.[57] Disinformation actors can use generative AI along with other automated techniques (including social bots) to create content and

54. Sun, *supra* note 10, at 375.

55. *See, e.g.*, Twitter, Inc. v. Taamneh, 598 U.S. 471, 481 (2023); Gonzalez v. Google LLC, 598 U.S. 617, 621 (2023).

56. *Taamneh*, 598 U.S. at 482; *Gonzalez*, 598 U.S. at 622.

57. *See, e.g.*, Press Release, FTC, FTC Announces Crackdown on Deceptive AI Claims and Schemes (Sept. 25, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes; Press Release, U.S. Treasury Financial Crimes Enforcement Network, FinCEN Issues Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions (Nov. 13, 2024), https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial; Blake Hall, *How AI-Driven Fraud Challenges the Global Economy—and Ways To Combat It*, WORLD ECON. FORUM (Jan. 16, 2025), https://www.weforum.org/stories/2025/01/how-ai-driven-fraud-challenges-the-global-economy-and-ways-to-combat-it; Press Release, FBI San Francisco, FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence (May 8, 2024), https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence.

interactions that deceptively appears to be posted by or involve real human beings.[58]

The internet and AI have exploded the risks of personal data privacy exposure, which in turn has drastically changed the disinformation landscape. Fueled by personal data, personalization exacerbates the harms of disinformation. Having established that personalization is the crux of the disinformation problem, Part III turns to solutions—both solutions that do not solve the problem and potential solution that might.

III. DISINFORMATION SOLUTIONS THAT DON'T SOLVE

This Article explained the problem with modern disinformation and introduced the concept of personalized disinformation—disinformation fueled by the vector of personalization. Now, the Article turns to two proposed solutions to disinformation (speech regulation and economic regulation) that do not solve the problem, before recommending a third solution (privacy regulation) that just might do the trick.

A. WHY SPEECH REGULATION IS A POOR SOLUTION

Governments may attempt to mitigate the harms of disinformation through speech regulation, either regulating the speech of individuals or regulating the speech of platform companies that host content posted by individuals. At first, such regulation of content would appear to be a natural fit, as speech governance is a regular government function. However, as this Subpart will show, speech regulation is a poor solution for disinformation because it is legally and politically untenable and unpopular with the public. Speech restrictions also create risks to civil liberties and democracy.

Speech regulation is a poor solution for disinformation for a number of reasons. Empowering the government to restrict individual speech is dangerous, as it creates greater risks for censorship and violations of critical civil liberties. Free speech is necessary for a democracy to survive, so we must proceed with extreme caution any time someone recommends a restriction on speech for a problem that could be solved better otherwise. Regulating speech through the proxy of regulating companies' content moderation practices is also dangerous, as it hides the state's actions from the public.[59] This leads to a lack of accountability, making it difficult for individuals to exercise their rights.

Individuals would do well to be skeptical of even the best-intentioned government actors who seek to control the flow of speech online, even if that speech is related to disinformation. After all, once precedent is created that allows government actors to police speech, it is difficult to roll back these powers. Some people might trust certain government actors (perhaps from one

58. *See* Bontridder & Poullet, *supra* note 48, at 5.

59. Daphne Keller, *Who Do You Sue? State and Platform Hybrid Power Over Online Speech* 4 (Hoover Inst., Aegis Series Paper No. 1902, 2019), https://www.hoover.org/research/who-do-you-sue.

presidential administration or one political party) to act responsibly when given legal authorities to censor speech online. However, assuming our democracy persists and term limits still exist in the future, no President or party is in office forever. It is naïve to imagine that all future government actors in the United States will be well-meaning, competent, and responsible enough to be entrusted with more powers than they already have to control and regulate speech. Thus, increasing the government's power to regulate speech is a risky gambit, even if the desired outcome is to stop disinformation.

Attempts to curb disinformation through speech regulation will often fail due to the strength of the U.S. Constitution's First Amendment. The United States Supreme Court has repeatedly upheld speech rights involving many kinds of false or otherwise harmful speech. In *Brandenburg v. Ohio*, the Court upheld the right for Ku Klux Klan members to engage in hate speech.[60] In *Snyder v. Phelps*, the Court decided that the Westboro Baptist Church was allowed to display signs with slurs against the LGBTQ community at a funeral for a gay man.[61] In *Virginia v. Black*, the Court held that a law banning the burning of crosses (a well-known hate symbol) was overly broad.[62] In *Sorrell v. IMS Health*, the Court held in favor of the First Amendment protecting advertising-related speech that included potentially sensitive health information.[63] In *United States v. Alvarez*, the Court reaffirmed its stance that even false speech can be protected under the First Amendment, striking down a statute that made it unlawful to falsely claim one had received military honors.[64] Even though one might consider disinformation to be false or harmful speech, it still is, at the end of the day, speech that is protectable under the First Amendment. Attempting to stop disinformation through speech regulation is likely to result in a constitutional violation.

Attempts to indirectly regulate speech by pressuring non-state actors, including social media companies, are also poor solutions for disinformation. One form of this indirect government regulation of speech is what some refer to as "jawboning."[65] Jawboning is the practice of government actors influencing private actors through indirect, extralegal means.[66] In lieu of directly regulating disinformation through speech laws or clear, public state action, governments can sometimes turn to other means, including indirect pressuring through jawboning. For example, instead of passing a law forcing technology corporations to minimize disinformation, elected representatives could give speeches on the harms that Big Tech corporations are creating by not limiting disinformation. This could influence companies to act on the issue, for fear of

60. Brandenburg v. Ohio, 395 U.S. 444, 449 (1969).
61. Snyder v. Phelps, 562 U.S. 443, 459–60 (2011).
62. Virginia v. Black, 538 U.S. 343, 347–48 (2003).
63. Sorrell v. IMS Health, Inc., 564 U.S. 552, 557 (2011).
64. United States v. Alvarez, 567 U.S. 709, 715 (2012).
65. *See, e.g.*, Derek E. Bambauer, *Against Jawboning*, 100 MINN. L. REV. 51, 55 (2015).
66. *Id.*

retaliation from Congress. Jawboning itself creates thorny legal problems, including constitutional problems with state actors exceeding legal authority.

Alleged jawboning was at the heart of *Murthy v. Missouri*, a 2024 Supreme Court case in which multiple states sued members and agencies of the Biden Administration, arguing impermissible government interference with speech.[67] Petitioners claimed the government had unlawfully pressured social media companies to censor information regarding conservative viewpoints, including anti-vaccine advocacy related to COVID-19 immunizations. While the Court ultimately decided the case on standing, eschewing thornier First Amendment questions, the facts of the case show how difficult it is for the U.S. government to attempt to regulate disinformation and propaganda, online and off. Indirect speech regulation is not a good solution for disinformation either.

Constitutional issues aside, other legal problems make speech regulation a poor solution for disinformation. Speech regulatory enforcement aimed at penalizing companies for hosting online disinformation may run into legal issues related to Section 230,[68] the law that provides a measure of legal immunity for some internet intermediaries regarding liability for user-generated content.[69] In what United States Naval Academy Professor Jeff Kosseff has described as "the twenty-six words that created the internet,"[70] Section 230(c)(1) states: "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[71] Section 230 prevents companies from being held responsible for the actions or speech of their users, including speech that may include disinformation. States that wish to impose penalties on corporations that host user-generated disinformation will find that difficult, due to the protections of Section 230.

Attempting to regulate disinformation through direct or indirect speech regulation pushes technology companies into an impossible position. If the companies are to regulate speech *ex ante*, they run the risk of over-censoring user speech. If they merely regulate speech *ex post*, they run the risk of allowing too much harmful content to spread. Government actors who seek to regulate speech through these corporate intermediaries also assume the same risks. Stanford Law School Professor Evelyn Douek argues that piecemeal online speech regulation reflects a myopic view of content moderation[72] Instead, Professor Douek believes speech regulation should focus on a holistic, systems-

67. Murthy v. Missouri, 603 U.S. 43, 49 (2024).

68. 47 U.S.C. § 230.

69. *See, e.g.*, Eric Goldman, *The Ten Most Important Section 230 Rulings*, 20 TUL. J. TECH. & INTELL. PROP. 1, 3 (2017).

70. Jeff Kosseff uses this phrase as the title for his popular book, but others have referred to the law in this manner before him. *See generally* JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019).

71. 47 U.S.C. § 230(c)(1).

72. Evelyn Douek, *Content Moderation as Systems Thinking*, 136 HARV. L. REV. 526, 585 (2022).

based approach that incorporates a fuller understanding of the difficult, practical tradeoffs involved in social media content moderation. Utilizing a systems-based approach should include acknowledgement of the role of AI and the internet in changing speech regulation generally, as well as the concept of personalized disinformation. Regulators must evaluate the tradeoffs of speech regulation solutions. As the tradeoffs are difficult and the harms to speech are many, regulators ought to focus on privacy regulation solutions that attack the vector of personalization of disinformation.

Speech regulation is not only a threat to democracy—it is also constitutionally and legally difficult. What's worse, it is deeply unpopular with the public. Even relatively limited, seemingly benign attempts to regulate disinformation as speech can lead to public backlash. For example, in 2022, the Biden Administration attempted to launch a new Disinformation Governance Board, an initiative hosted by the Department of Homeland Security.[73] This Board was set to study and respond to disinformation, a relatively normal government function. After all, other government agencies, including offices with intelligence or security functions, already study and respond to disinformation. However, the rollout of the Board met enormous resistance from the public as well as political pushback from lawmakers.[74] Pushback included coordinated harassment attacks against the proposed head of the board, disinformation expert Nina Jankowicz.[75] Eventually, Homeland Security pulled back on the initiative, and the Disinformation Governance Board was disbanded before it began.[76] University of Louisville Professor of Law Russell L. Weaver argues that the concept of a Disinformation Governance Board was, in and of itself, antithetical to American values of freedom of speech.[77] This is just one example of the unpopularity and political infeasibility of regulating disinformation through speech regulation.

Speech regulation is a poor solution for disinformation. It fails to resolve the personalization element of modern disinformation. Speech regulation is also not politically or legally tenable and, even when it is, runs the risk of causing serious, harmful consequences to autonomy, civil liberties, and democracy.

---

73. *Fact Sheet: DHS Internal Working Group Protects Free Speech and Other Fundamental Rights When Addressing Disinformation That Threatens the Security of the United States*, DEP'T HOMELAND SEC. (May 2, 2022), https://www.dhs.gov/archive/news/2022/05/02/fact-sheet-dhs-internal-working-group-protects-free-speech-other-fundamental-rights.

74. Tiffany C. Li, *Mayorkas' Botched DHS Disinfo Rollout Pinpoints a Weakness of American Government*, MSNBC (May 5, 2022, at 4:07 PM PDT), https://www.msnbc.com/opinion/msnbc-opinion/biden-s-dhs-failure-exposes-government-weak-spot-n1295188.

75. Cristiano Lima-Strong, *DHS Tries To Right Controversial Rollout of Its 'Disinformation Governance Board'*, WASH. POST (May 2, 2022), https://www.washingtonpost.com/politics/2022/05/02/dhs-tries-right-controversial-rollout-its-disinformation-governance-board.

76. *Id.*

77. Russell L. Weaver, *Remedies for "Disinformation"*, 55 U. PAC. L. REV. 185, 203 (2024).

B. WHY ECONOMIC REGULATION IS A POOR SOLUTION

Economic regulation is also a poor solution to combat disinformation. By economic regulation, this Article refers specifically to proposed solutions that focus on regulating the market for technologies that can be used to create or spread disinformation. Such economic regulation does not address the personalization at the root of modern disinformation and can cause backlash among American consumers as well as tensions abroad.

Economic regulation has been proposed as a solution for disinformation in a number of ways. President Trump first attempted to ban TikTok via executive order during his first term.[78] In his first executive order on the subject, Trump noted that applications owned by Chinees companies threatened "the national security, foreign policy, and economy of the United States."[79] The executive order also stated that TikTok "may also be used for disinformation campaigns that benefit the Chinese Communist Party, such as when TikTok videos spread debunked conspiracy theories about the origins of the 2019 Novel Coronavirus."[80] In a follow-up executive order, Trump ordered ByteDance to divest itself of all TikTok-related assets in the United States.[81]

Banning TikTok can be considered economic regulation, though there is also an argument for a TikTok ban as being primarily a national security regulation, with incidental economic benefits.[82] Despite the national security claims, the executive order's regulatory enforcement came through a ban on transactions with ByteDance, TikTok's parent company, as well as an order for the company to divest its assets. Thus, effectively, this ban was a market economic regulation.

The various efforts to ban TikTok by regulating its parent company's role in the market have proven ineffective. Another form of economic regulation offered as a disinformation solution involves regulating the market for social media or content platforms. The first Trump executive order on TikTok in 2020 made it unlawful to engage in transactions with ByteDance. This move would have affected companies like Apple and Google, which offered the app on their app stores. It would also have affected companies and individuals who paid for

78. Bobby Allyn, *Trump Signs Executive Order That Will Effectively Ban Use of TikTok in the U.S.*, NPR (Aug. 6, 2020, at 11:21 PM ET), https://www.npr.org/2020/08/06/900019185/trump-signs-executive-order-that-will-effectively-ban-use-of-tiktok-in-the-u-s.

79. *Executive Order on Addressing the Threat Posed by TikTok*, TRUMP WHITE HOUSE ARCHIVES (Aug. 6, 2020), https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok.

80. *Id.*

81. *Trump Orders Chinese Owner of TikTok to Sell US Assets*, ASSOCIATED PRESS (Aug. 14, 2020, at 6:18 PM PDT), https://apnews.com/article/ap-top-news-technology-foreign-policy-politics-business-1f636191b0b9e28c7041fb64fb547801.

82. One counter-argument may be as follows: TikTok is dangerous for national security, as it creates cybersecurity vulnerabilities on American devices, leaks private American data to China (data which could be used to harm national security interests), and creates a speech environment where China can manipulate the content that Americans view, in order to disinform or spread propaganda.

subscriptions or advertising services on the application. Restricting companies who offer social media or content applications to users can also be considered economic regulation.[83] Regulations that target app store companies, as well as internet infrastructure companies, can also arguably be considered speech regulations—but the law is not clear.[84] The repeated political failure to ban TikTok shows the difficulty with using economic regulation to regulate disinformation.

Economic regulation of disinformation that include bans of applications being used by Americans will likely prove unpopular. Not only are Americans rightly concerned about speech censorship, but generally, people do not like when things they enjoy are taken away from them. TikTok is a popular application. A 2024 Pew study found that thirty-three percent of American adults use TikTok, including fifty-nine percent of adults aged eighteen to fifty-nine years old.[85] The app is even more popular among teens, with sixty-three percent of American teenagers aged thirteen to seventeen using the application, including fifty-seven percent who use it daily.[86]

To be sure, the popularity of the application does raise concerns regarding disinformation as well as privacy. The application is owned by a Chinese company, ByteDance.[87] Though that company claims the U.S. subsidiary is independent, investigations have revealed multiple instances of personal data making its way back to China.[88] It is possible that the Chinese government could exert influence on TikTok, which could lead to more disinformation reaching American audiences. This is especially concerning, as seventeen percent of all U.S. adults claim to regularly consume news on TikTok.[89] However, attempts to mitigate disinformation harms from TikTok that rely on banning TikTok have been and likely will continue to be unpopular, as long as the application is popular among the American public.

---

83. *See, e.g.*, John M. Yun, *App Stores, Aftermarkets, & Antitrust*, 53 ARIZ. ST. L.J. 1283, 1285–86 (2021).

84. *See, e.g.*, Bridy, *supra* note 27, at 195–96; Laura DeNardis & Francesca Musiani, *Governance by Infrastructure*, *in* THE TURN TO INFRASTRUCTURE IN INTERNET GOVERNANCE 1, 3 (Francesca Musiani, Derrik L. Cogburn, Laura DeNardis & Nanette S. Levinson eds., 2014); David G. Post, *Internet Infrastructure and IP Censorship*, IP JUST. J., Aug. 1, 2015, at 1, 15.

85. Kirsten Eddy, *8 Facts About Americans and TikTok*, PEW RSCH. CTR. (Dec. 20, 2024), https://www.pewresearch.org/short-reads/2024/12/20/8-facts-about-americans-and-tiktok/.

86. *Id.*

87. *See* He, *supra* note 1.

88. Simon Sharwood, *US Claims TikTok Shipped Personal Data to China–Very Personal Data*, REG. (Jul. 29, 2024, at 4:29 AM UTC), https://www.theregister.com/2024/07/29/doj_tiktok_filing_china_data/; Haleluya Hadero, *TikTok Is Under Investigation by the FTC Over Data Practices and Could Face a Lawsuit*, ASSOCIATED PRESS (Mar. 27, 2024, at 9:57 AM PDT), https://apnews.com/article/tiktok-ftc-investigation-china-data-e91e02db5c4f3f7d5836ecafedbf4714; Emily Baker-White, *Leaked Audio from 80 Internal TikTok Meetings Shows that US User Data Has Been Repeatedly Accessed From China*, BUZZFEED NEWS (Jun. 17, 2022, at 9:31 AM), https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access.

89. Eddy, *supra* note 85.

Thus, banning TikTok has proven to be politically untenable and unpopular with the public. President Trump first threatened to ban TikTok via executive order during his first term, an announcement that caused backlash from the public.[90] The public backlash may have been part of the reason President Trump eventually delayed the executive orders' effects until he was out of office, and part of the reason Biden refrained from enforcing the executive order through his term as well.

In 2024, Congress passed (and President Biden signed) the Protecting Americans from Foreign Adversary Controlled Applications Act ("PAFACAA"), which made it unlawful to "[provide] services to distribute, maintain, or update [a] foreign adversary controlled application" like TikTok.[91] This led to a lawsuit heard by the Supreme Court, which eventually found the ban lawful.[92] This law again caused backlash, which amusingly included a spate of Americans downloading the Chinese-owned, Chinese-language social media application Xiahongshu (translated as Little Red Book or Red Note).[93]

Economic regulations that seek to control disinformation by targeting foreign companies may threaten U.S. international relations and foreign policy objectives. Not only did the TikTok ban create backlash among the American public, but it also generated ill will with the Chinese government. After the law was passed, the Chinese foreign ministry referred to the actions of the U.S. as "an act of bullying," and argued that the U.S. was engaging in unfair trade practices. [94] Though the law banning TikTok eventually proved so unpopular it was delayed through executive order,[95] the Chinese Foreign Ministry still protested America's actions as unfair.[96] While not every economic regulation seeking to target disinformation will disproportionately affect a foreign company, those that do will run into international relations and trade problems.

The unpopularity of economic regulations that seek to control disinformation by controlling applications is important because unpopularity with the public and with the international community can make such regulations

---

90. Jill Colvin & Barbara Ortutay, *From Backing a Ban to Being Hailed as a Savior: Inside Trump's TikTok Shift*, ASSOCIATED PRESS (Jan. 19, 2025, at 7:22 PM PDT), https://apnews.com/article/trump-tiktok-ban-da11df6d59c17e2c17eea40c4042386d.

91. Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, 138 Stat. 895, 955–56 (2024).

92. TikTok, Inc. v. Garland, 604 U.S. 56, 72 (2025).

93. Fu Ting & David Cohen, *TikTok Refugees Are Pouring to Xiaohongshu. Here's What You Need to Know About the RedNote App*, ASSOCIATED PRESS (Jan. 17, 2025, at 4:55 PM PDT), https://apnews.com/article/tiktok-refugee-xiaohongshu-rednote-855692624aa52825b30afc5474af881d; *Everything You Need to Know About Xiaohongshu*, REST OF WORLD (Jan. 15, 2025), https://restofworld.org/2025/rednote-xiaohongshu-what-to-know.

94. Nectar Gan, Marc Stewart & Wayne Chang, *China Says US TikTok Ban 'An Act of Bullying' That Would Backfire*, CNN (Mar. 13, 2024, at 11:18 PM EDT), https://www.cnn.com/2024/03/13/business/china-tiktok-ban-bullying-congress-vote-intl-hnk/index.html.

95. Note that executive orders cannot overturn acts of Congress.

96. Simone McCarthy, *Trump Has Tossed TikTok a Lifeline. But China's Not Happy,* CNN (Jan. 21, 2025, at 3:29 AM EST), https://www.cnn.com/2025/01/21/tech/trump-tiktok-china-intl-hnk/index.html.

difficult to enforce legally. For example, by the time the decision was nearing publication, Congress had already indicated reluctance to support the law.[97] When Trump returned to office in January 2025, he announced he would not proceed with the TikTok ban, signing an executive order with the intention to delay the law's effects.[98] While an executive order cannot legally undo an act of Congress, it does point to the political unpopularity of banning TikTok. The ongoing TikTok debacle shows the political infeasibility of solving disinformation through economic regulations that focus on preventing or limiting the free market.

In general, economic regulation solutions for disinformation are not only unpopular among the public, but they also harm core American values of a free market. Economic regulation can also create international trade and international relations problems, particularly as the U.S. publicly supports free market economies. This may occur especially if the U.S. government seeks to regulate only foreign-owned applications. Moreover, any solutions that limit the ability for individuals to access and use the applications they wish will also harm rights to speech and autonomy. Instead, lawmakers should focus on privacy regulations that target the vector of personalization in disinformation, as privacy regulations are unlikely to come with the same negative consequences and harms of economic regulation proposed to solve disinformation.

IV. PRIVACY LAW SOLUTIONS FOR DISINFORMATION

This Article has explained that the core of the problem with disinformation and propaganda on social media is personalization. Part III specifically highlighted why two commonly proposed solutions (speech regulation and economic regulation) are inadequate and also harmful. This Article now proposes an alternative solution that will actually address the crux of the problem, without the same harmful externalities. In short, lawmakers should turn to privacy regulation to solve for the personalization vector of disinformation.

Privacy regulation is the best solution for today's personalized disinformation problem, as Part IV will show through four main arguments: (1) privacy regulation solves for personalization by attacking the source of personalization on a technical level; (2) privacy regulation avoids constitutional roadblocks that would stymie speech regulation solutions; (3) privacy regulation avoids international relations and trade blowback that would come from economic or trade regulation solutions; and (4) privacy regulation would be less unpopular with the public, and thus more politically tenable than both speech regulation and economic regulation.

Privacy regulation is the best solution for modern disinformation because privacy laws can attack the source of personalization on a technical level.

97. Miranda Nazzaro, *Schumer Pushes for TikTok Ban Delay as Deadline Looms*, HILL (Jan. 16, 2025, at 2:04 PM ET), https://thehill.com/policy/technology/5089746-tiktok-ban-delay-schumer.

98. Colvin & Ortutay, *supra* note 90.

Privacy regulation can include limitations on the ability for public or private actors to collect, use, store, transfer, or sell personal information from individuals. Such limitations are already found in privacy regulations, including Europe's General Data Protection Regulation ("GDPR")[99] and California's consumer privacy statute, the California Consumer Privacy Act[100] (as amended by the California Privacy Rights Act).[101] These data limitations may restrict the ability for bad actors to create and target disinformation content and produce false interactions that have the potential to lead to extremist radicalization. Privacy regulations could also incorporate restrictions on automated data processing or provisions on the use of data for AI generally.[102] This could also weaken the ability for bad actors to use AI to personalize and spread disinformation. Neither speech nor economic regulation attack the heart of personalization, which is why data privacy regulation is a better solution than both.

Another reason why privacy regulation is the best solution is because privacy law avoids constitutional roadblocks that have plagued speech regulation proposals that target false or harmful online content. While privacy is a constitutional right,[103] the right to privacy in America arguably pales in comparison to the right to freedom of speech. The U.S. is well-known to be a speech maximalist country, and the courts tend to weigh free speech far above other competing values. Many government efforts at regulating speech online, including regulating disinformation, will fail because courts will find that such speech regulations constitute impermissible government restrictions on constitutionally protected speech, as discussed earlier in this Article. Privacy regulation can avoid implicating First Amendment concerns.

Privacy regulation is also the best solution for disinformation given the context of international relations. Economic regulation seeking to curb disinformation could run into international trade and international relations problems, especially if such regulation disproportionately affects foreign-owned technology corporations. This unequal application of disinformation-focused economic regulations may occur as the U.S. government becomes more skeptical of foreign-owned applications that can spread disinformation, when

99. 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, art. 5, 2016 O.J. (L 119) 1, 35.

100. CAL. CIV. CODE § 1798.100 (West 2025).

101. CAL. CIV. CODE §§ 1798.100–99 (West 2025) (amended 2020).

102. Such restrictions can be found in the GDPR as well. *See* Regulation (EU) 2016/679, art. 22, 2016 O.J. (L 119) 1, 46.

103. The U.S. Constitution has no explicit right to privacy, but the Supreme Court has recognized a right to privacy as emanating from the penumbra (or shadows) of the Bill of Rights, particularly related to due process and fundamental rights. Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965). However, the Court's recent decision in *Dobbs v. Jackson Women's Health Org.* casts some doubt on the continued viability of the penumbra interpretation of constitutional privacy rights. 597 U.S. 215, 231 (2022); *see, e.g.*, Tiffany C. Li, *State Constitutional Rights to Privacy*, GA. L. REV. (forthcoming 2025) (manuscript at 3).

compared to U.S.-owned applications, even if both may spread disinformation. At least with U.S.-owned companies, the U.S. government has more direct means of exerting control and imposing penalties.

The TikTok example shows the difficulties economic regulation of disinformation can create in an international context. After Congress passed the TikTok ban, the Chinese foreign ministry called the law "an act of bullying."[104] They alleged unfairness in international economic competition. Even after President Trump signed his executive order attempting to delay the legal ban of TikTok,[105] the Chinese Foreign Ministry still expressed unhappiness regarding America's actions generally.[106] Economic regulations that disproportionately restrict foreign-owned applications run the risk of upsetting other nations and the international community, as these regulations may be seen as unfair economic protectionism.

Privacy regulation would be best for international relations because passing a privacy law would finally bring the U.S. in line with many other jurisdictions who have already passed privacy laws, including the European Union, the United Kingdom, Canada, Japan, and China.[107] This could help prove America's willingness to stand together with other nations in creating norms of privacy to protect international conceptions of human rights generally.[108]

Finally, privacy regulation would also be the most popular solution for disinformation. Americans care about privacy rights, and it is likely that Americans would support the passing of a federal privacy law. A 2023 Publishers Clearing House survey showed that eighty-six percent of Americans are concerned about privacy and security of personal information.[109] A 2022 Morning Consult and Politico poll found that over half of Americans would support a national privacy law.[110] Another 2024 Consumer Reports survey found that seventy-eight percent of Americans would support a privacy law.[111]

104. *See* Gan et al., *supra* note 94.

105. As a reminder, executive orders cannot overturn acts of Congress.

106. *See* McCarthy, *supra* note 96.

107. Tiffany C. Li, *Post-Pandemic Privacy Law*, 70 AM. U. L. REV. 1681, 1718 (2021).

108. To be fair, an argument could be made that regulating disinformation through speech regulation would also put the U.S. more in line with much of the international community, as the U.S. is a relative outlier in terms of free speech protections. Many other countries allow government actions to censor speech, especially speech that is harmful or false. However, due to the unique cultural and historical factors that have created our free speech maximalist culture, it is unlikely the U.S. (or the American people) will favor stronger speech regulation to bring us in line with other nations.

109. PUBLISHERS CLEARINGHOUSE, TIFFANY JOHNSON, N.Y.U., DANIELA MOLTA, SYRACUSE UNIV. & EVAN SHAPIRO, IT'S ALL PERSONAL: A STUDY ON CONSUMER ATTITUDES TOWARDS DATA COLLECTION AND USAGE 5 (2023), https://www.tvrev.com/special-reports/p/its-all-personal-a-study-on-consumer-attitudes-towards-data-collection-usage.

110. Chris Teale, *More Than Half of Voters Back a National Data Privacy Law*, MORNING CONSULT (Jan. 12, 2022, at 6:00 AM UTC), https://pro.morningconsult.com/instant-intel/federal-data-privacy-legislation-polling.

111. Scott Medintz, *Americans Want Much More Online Privacy Protection Than They're Getting*, CONSUMER REPS. (Nov. 20, 2024), https://www.consumerreports.org/electronics/privacy/americans-want-much-more-online-privacy-protection-a9058928306.

Nineteen states have passed privacy laws thus far, and it is likely that more will join the trend. This highlights the political feasibility of passing privacy laws. A privacy regulation would not only respond to the personalization factor of disinformation, but it would be popular as well. At the very least, a privacy regulation solution would be more popular than speech or economic regulation.

For these reasons, privacy regulation is the best solution for combatting disinformation, given the personalized nature of disinformation in today's information society. Instead of wasting time on speech regulations that will not pass constitutional muster, or economic regulations that will be unpopular both in the U.S. and abroad, lawmakers should focus efforts on passing a federal privacy law that will regulate the personalization vectors of disinformation.

CONCLUSION

This Article provided a holistic overview of three forms of proposed solutions for disinformation—speech, economic, and privacy regulation—and evaluated each in terms of ability to solve the personalized disinformation issue as well as other practical drawbacks and benefits.

Part I began by explaining disinformation and its harms, and then proceeded to showcase how the internet and AI have changed the information sphere—as well as pathways of disinformation. The rise of the internet and AI have changed disinformation by making it increasingly personalized, fueled by the personal data collected from individuals on the internet. Thus, personalization has become the crux of the disinformation problem. Unfortunately, current proposed solutions for disinformation (speech regulation and economic regulation) fail to solve for the personalization dimension of disinformation.

Both speech and economic regulations are poor solutions to combat disinformation. Speech regulations are dangerous for democracy, legally and constitutionally untenable, and deeply unpopular with the public. For example, recent Supreme Court decisions in *Taamneh*[112] and *Gonzalez*[113] show the limits of speech regulation to counter disinformation online. Economic regulations are unpopular with the public and international community, and threaten core American values of a free market. For example, the public backlash and immediate walking back of the TikTok ban shows the limits of economic regulation of disinformation.

Instead, lawmakers should turn to privacy and data protection regulation, which will attack the personalization vector of disinformation, without the negative externalities of speech or economic regulation. Privacy regulation attacks the source of personalization on a technical level and is the only solution that takes into account the impact of the internet and AI on the modern

112. Twitter, Inc. v. Taamneh, 598 U.S. 471 (2023).

113. Gonzalez v. Google, LLC, 598 U.S. 617 (2023).

disinformation landscape. Privacy regulation would be more legally and constitutionally defensible, and better for international relations and foreign policy purposes. Privacy regulation would also likely be popular with the public, or at least *less unpopular* with the public.

Privacy regulation is the best solution to combat modern disinformation. Of course, in this time of political uncertainty, it is unclear if Congress will find the motivation to finally pass a national privacy law. However, U.S. lawmakers should strongly consider pushing through such a law to protect the American people from the harms of privacy invasions and the nation from the harms of personalized disinformation. Additionally, finally passing a national privacy law would be a foreign policy win that would bring the U.S. in line with the rest of the world[114] and help the U.S. shape global norms of privacy and speech.[115]

As personalization is the new lynchpin for modern disinformation, this Article argues that lawmakers should focus on solving for personalization and highlights why speech and economic regulation will not solve personalized disinformation problems. If lawmakers are serious about solving the disinformation problem, they must attack the core of the problem: personalization, fueled by the internet and AI. Neither speech nor economic regulation will solve the personalized disinformation crisis. Only privacy regulation will.

114. *See* Li, *supra* note 107.

115. At time of writing, it is unclear if the U.S. has any interest in participating in the international community or if the country will be seen at all as a legitimate, good faith participant in the building of global democratic norms. But that is a topic for another day.

***