

2023

Protecting Public Health Amidst Data Theft, Sludge, and Dark Patterns: Overcoming the Constitutional Barriers to Health Information Regulations

Jon M. Garon

Follow this and additional works at: <https://ideaexchange.uakron.edu/akronlawreview>



Part of the [Intellectual Property Law Commons](#)

Please take a moment to share how this work helps you [through this survey](#). Your feedback will be important as we plan further development of our repository.

Recommended Citation

Garon, Jon M. (2023) "Protecting Public Health Amidst Data Theft, Sludge, and Dark Patterns: Overcoming the Constitutional Barriers to Health Information Regulations," *Akron Law Review*. Vol. 56: Iss. 2, Article 1.

Available at: <https://ideaexchange.uakron.edu/akronlawreview/vol56/iss2/1>

This Article is brought to you for free and open access by Akron Law Journals at IdeaExchange@Uakron, the institutional repository of The University of Akron in Akron, Ohio, USA. It has been accepted for inclusion in Akron Law Review by an authorized administrator of IdeaExchange@Uakron. For more information, please contact mjon@uakron.edu, uapress@uakron.edu.

**PROTECTING PUBLIC HEALTH AMIDST DATA THEFT,
SLUDGE, AND DARK PATTERNS: OVERCOMING THE
CONSTITUTIONAL BARRIERS TO HEALTH INFORMATION
REGULATION**

*Jon M. Garon**

Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.

— Justice Louis D. Brandeis**

Knowing is not enough; we must apply.

Willing is not enough; we must do.

— Johann Wolfgang von Goethe

I.	Introduction	180
II.	Key Components and Vulnerabilities to the Health Infosystem	182
	A. HIPAA Protected Information and Cyberattacks	183
	B. Personal Health Information Not Protected by HIPAA 187	
	C. The Exacerbating Threat of Misinformation and Disinformation	194
III.	Individual Autonomy in Health Care and Health Information Versus the Threats of Sludge and Dark	

*Professor of Law and Director, Intellectual Property, Cybersecurity, and Technology Law program, Nova Southeastern University Shepard Broad College of Law. Earlier versions of this paper were presented at the Center for Intellectual Property Law & Technology annual IP Scholars Forum, University of Akron School of Law (Dec. 2022) and the Thirteenth Annual Loyola Constitutional Law Colloquium, cosponsored by Chicago Loyola and George Washington School of Law Nov. 2022). The author wishes to extend special thanks for insights and feedback from Mark F. Schultz, Sandra Aistars, Mark A. Cohen, Alexandra George, Camilla Hrdy, Willajeanne McLean, Emily Michiko Morris, Craig Nard, Cesar-Joel Ramirez-Montes, and Guy Rub.

** Louis D. Brandeis, *What Publicity Can Do*, HARPER'S WEEKLY 10 (December 20, 1913), <https://books.google.com/books?id=-WktAQAAAMAJ&q=%22of+disinfectants%22#v=snippet&q=%22of%20disinfectants%22&f=false> [https://perma.cc/2SGE-SF5T].

	Patterns.....	201
IV.	The FTC’s Role in Policing Unfair and Deceptive Trade Practices.....	210
V.	Limits on Health Care Information Reform: Commercial Free Speech Jurisprudence	222
VI.	Regulating the User Experience	229
VII.	Reclaiming the Marketplace of Health information From Disinformation.....	232
VIII.	Conclusion.....	238

I. INTRODUCTION

In 2017, popular health blogger Belle Gibson was fined \$410,000 (Australian Dollars) for a campaign she perpetrated using her blog and phone apps in which the young, vivacious blogger wrote about curing her multiple forms of cancer, including an incurable brain tumor, by eating whole foods. Gibson spun out her increasingly incredible story on her blog, her fictionally autobiographical book entitled “The Whole Pantry,” and an accompanying smartphone app.¹ As the prosecution for violations of Australian consumer protection law determined, Gibson never suffered from cancer. In addition, many of the financial claims she made were used to defraud donors who thought they were contributing to the medical expenses of other cancer victims.²

A very different form of health care fraud was suffered by Anndorie Cromar.³ Her health care information was stolen and used by another woman to receive maternity care. The imposter’s infant was born with drugs in the baby’s system, leading to an intervention by child protective services. Cromar, who had no idea that her identity was stolen, was required to submit DNA evidence to exonerate her from the claims of

1. Elizabeth Pratt, *Fake Blogs: Warnings About Medical Advice from Online ‘Experts’*, HEALTHLINE (Oct. 19, 2017), <https://www.healthline.com/health-news/fake-blogs-warning-about-medical-advice-from-online-experts> [https://perma.cc/BWA3-3TEZ]; Libby-Jane Charleston, *‘Health Guru’ Faker Belle Gibson Fined \$410,000 For Lying About Cancer Cure*, HUFFPOST (Sept. 27, 2017), https://www.huffpost.com/archive/au/entry/health-guru-faker-belle-gibson-fined-410-000-for-lying-about-cancer-cure_a_23225383 [https://perma.cc/7SDM-3U8H].

2. See Charleston, *supra* note 1 (“Shortly after her book was released, it was revealed that Gibson never had brain cancer, or any other disease. There were also many allegations that the charities she claimed had received money, never received a cent.”).

3. See Michelle Andrews, *The Rise of Medical Identity Theft*, CONSUMER REPORTS (Aug. 25, 2016), <https://www.consumerreports.org/health/medical-identity-theft-a1699327549/> [https://perma.cc/A4LE-D8FM].

child endangerment and retain the custody of her own four children.⁴ Medical identity theft also led to the arrest of Deborah Ford.⁵ Her purse was stolen. She promptly reported the theft to police, cancelled her credit card, and even had a new driver's license issued. But over the next two years, the medical insurance information stolen from her purse had been used to purchase "more than 1,700 prescription opioid painkiller pills through area pharmacies."⁶ Her compromised data was a link in the chain supporting the nationwide opioid crisis and only her timely police report kept her from being arrested as part of the massive fraudulent conspiracy.⁷

Health care fraud takes many forms, but pervasive misinformation, intentional disinformation, data mismanagement, cybertheft, and poor patient protection each play a significant role in the overall failure to protect individual patients from medical and financial harm, as well as failing to protect the nation's public health system from massive amounts of fraud and abuse. Individuals follow bad advice, receive deceptive information on how to protect their health, and can even lose access to health services. At the public health level, "studies find that exposure to misinformation can undermine vaccination uptake and compliance with public-health guidelines."⁸

This article first identifies the key components and vulnerabilities to the health infosystem. The article then identifies how the current model of partial and overlapping regulations leaves patients and the public vulnerable to fraud and abuse. It also explores the extent to which the individual's right to autonomy in health care must be incorporated into the system of information regulation. The next section reviews the current regulatory regime and its needs for reform. These reform goals are then assessed against the recent changes to commercial free speech jurisprudence and the constitutional limitations being placed by the Supreme Court on these necessary reforms. Finally, the paper suggests modifications to the regulatory approach by state and federal officials that may assuage some of the Supreme Court's ideological limitations on effective health care regulation. In addition to promoting regulatory enforcement against misuse of health data and the promotion of information designed to defraud the public, the article calls for a significant investment in the creation of a public health information

4. *Id.*

5. *Id.*

6. *Id.*

7. *Id.*

8. Sander van der Linden, *Misinformation: susceptibility, spread, and interventions to immunize the public*, 28 *NATURE MEDICINE* 460, 460 (2022).

network so that accurate and timely public health information and wellness information is part of the marketplace of health knowledge.

II. KEY COMPONENTS AND VULNERABILITIES TO THE HEALTH INFOSYSTEM

The consumer fraud perpetrated by Belle Gibson with her fictional cancer story reflects a clear abuse of public trust by sharing health information as a way to engage in a community of people suffering from significant medical issues and then exploiting those individuals for commercial gain. Disinformation is often quite compelling. Gibson's "app was downloaded 200,000 times within the first month, voted Apple's Best Food and Drink App of 2013 and ranked #1 in the App store."⁹ In other cases, such as those experienced by Anndorie Cromar and Deborah Ford,¹⁰ the consumer fraud is initiated by a data breach or data theft. "Whether the attack vector is ransomware, credential harvesting or stealing devices, the healthcare industry is a prime target for attackers to monetize PHI and sell on the Dark Web or hold an entity ransom unable to deliver patient care."¹¹ In addition, other risks come from the inside, as health care providers themselves find ways to monetize patient data and circumvent privacy protections.¹² Each of these three disparate risks—cybersecurity breaches, HIPAA avoidance, and disinformation—combine to place public health at unnecessary risk.

9. Briony Swire-Thompson & David Lazer, *Public Health and Online Misinformation: Challenges and Recommendations*, 41 ANNUAL REVIEW OF PUBLIC HEALTH 433, 437 (2020).

10. See Andrews, *supra* note 3.

11. Heather Landi, *Healthcare data breaches hit all-time high in 2021, impacting 45M people*, FIERCE HEALTHCARE (Feb. 1, 2022, 5:00 PM), <https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people> [<https://perma.cc/38XQ-4MCG>] (quoting statement of John Delano, healthcare cybersecurity strategist at Critical Insight and vice president at Christus Health).

12. See, e.g., Tatum Hunter & Jeremy B. Merrill, *Health apps share your concerns with advertisers. HIPAA can't stop it*, WASH. POST (Sept. 22, 2022), <https://www.washingtonpost.com/technology/2022/09/22/health-apps-privacy/> [<https://perma.cc/5JAT-ADHE>] ("[S]ending user identifiers along with key words from the content we visit opens consumers to unnecessary risk. Big data collectors such as brokers or ad companies could piece together someone's behavior or concerns using multiple pieces of information or identifiers."); Geoffrey A. Fowler, *You agreed to what? Doctor check-in software harvests your health data*, WASH. POST (June 13, 2022, 5:00 AM), <https://www.washingtonpost.com/technology/2022/06/13/health-privacy/> [<https://perma.cc/3TZ8-AJCK>] ("There's a burgeoning business in harvesting our patient data to target us with ultra-personalized ads.").

A. *HIPAA Protected Information and Cyberattacks*

The theft of health care data is the most obvious example of criminal behavior that targets the health care sector. Although cyberattacks impact all aspects of the economy, the financial harm is highest in the health care sector.¹³ These attacks are also exposing a record number of individuals to data exposure, with 45 million individuals being impacted in 2021 alone.¹⁴

But it is the nature of the health care infosystem that makes it uniquely vulnerable to these attacks and so many others. Ransomware attacks, for example, create the risk that hospitals or health care providers are shut down and incapable of providing medical services.¹⁵

“Hospitals have been hit pretty hard with high-impact ransomware attacks during the pandemic,” said John Riggi, national adviser for cybersecurity and risk at the American Hospital Association.

Riggi noted that during the pandemic, hospitals have had to rapidly expand network and internet-connected technology and deploy remote systems to support staffers who shifted to telework.

“The bad guys took advantage of that and had more opportunities to get into our networks,” he said.¹⁶

The impact also extends beyond the disruption and denial of medical services. “20% of medical identity fraud victims experience misdiagnosis and mistreatment.”¹⁷ Simply put, the harm caused by disinformation and disruption impact lives every day.

13. See Heather Landi, *Healthcare data breach costs reach record high at \$10M per attack: IBM report*, FIERCE HEALTHCARE (July 27, 2022), <https://www.fiercehealthcare.com/health-tech/healthcare-data-breach-costs-reach-record-high-10m-attack-ibm-report> [https://perma.cc/82XE-J9YA] (healthcare data breach costs average \$10.1 million, according to IBM Security’s annual Cost of a Data Breach Report surveying data breaches from March 2021 to March 2022. “That’s up 9.4% from the same timeframe a year earlier. Healthcare has had the highest breach-related financial damages for 12 consecutive years. . .”).

14. Landi, *supra* note 11.

15. Jenni Bergal, *Ransomware Attacks on Hospitals Put Patients at Risk*, STATELINE (May 18, 2022), <https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/05/18/ransomware-attacks-on-hospitals-put-patients-at-risk> [https://perma.cc/E2J3-ZS8K] (For example, a University of Vermont Medical Center “ransomware attack had forced officials to shut down all internet connections, including access to patients’ electronic health records, to prevent cybercriminals from doing any more damage.”).

16. *Id.*

17. *14 Gripping Medical ID Theft Statistics to Ponder on in 2022*, SAFEATLAST (Jan. 10, 2022), <https://safeatlast.co/blog/medical-id-theft-statistics/> [https://perma.cc/UU8S-WCCF].

At one level, health care information is among the most heavily regulated data in the U.S.¹⁸ The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), as amended by the Health Information Technology for Economic and Clinical Health Act (“HITECH”), provides a detailed mechanism for maintaining patient information.¹⁹ The comprehensive regulations that implement HIPAA include the Privacy Rule, the Security Rule, and the Breach Notification Rule.²⁰ The HIPAA Privacy Rule protects protected health information (“PHI”)²¹ from general disclosure unless used for treatment, payment, and health care operations, when provided to the individual, or in certain other limited circumstances.²²

The HIPAA Security Rule establishes highly prescriptive administrative, technical, and physical safeguards for protecting

18. See, e.g., Stacey A. Tovino, *The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons*, 47 SETON HALL L. REV. 973, 992 (2017) (“It would be tempting to say that the Privacy Rule is, across the board, more detailed and directive than the GDPR.”).

19. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936; Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified in scattered sections of 42 U.S.C.). See Jianyan Fang, *Health Data at Your Fingertips: Federal Regulatory Proposals for Consumer-Generated Mobile Health Data*, 4 GEO. L. TECH. REV. 125, 144 (2019) (“The most well-known federal statute for health data protection is HIPAA.”).

20. See Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000) (“The rule seeks to balance the needs of the individual with the needs of the society.”); *id.* at 82,468 (“The task of society and its government is to create a balance in which the individual’s needs and rights are balanced against the needs and rights of society as a whole.”); *id.* at 82,472 (“The need to balance these competing interests—the necessity of protecting privacy and the public interest in using identifiable health information for vital public and private purposes—in a way that is also workable for the varied stakeholders causes much of the complexity in the rule.”).

21. 45 C.F.R. § 160.103 (2022).

22. 45 C.F.R. § 164.502(a)(1) (2022). The U.S. Department of Health and Human Services (HHS) provides this summary of the mandatory and permissive disclosures:

Required Disclosures. A covered entity must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action. [45 C.F.R. § 164.502(a)(2).]

Permitted Uses and Disclosures. A covered entity is permitted, but not required, to use and disclose protected health information, without an individual’s authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of research, public health or health care operations. Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make. [45 C.F.R. § 164.502(a)(1).]

Summary of HIPAA Privacy Rule, U.S. HEALTH AND HUM. SERVS., <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> [<https://perma.cc/M94U-5L75>].

electronic health records (“e-PHI”).²³ The regulations which accompany HHS guidance provide detailed recommendations for applying appropriate data security and integrity policies, as well as imposing large financial penalties for failing to protect e-PHI data.²⁴

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. Specifically, covered entities must:

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.²⁵

The Health and Human Services Office of Civil Rights (“OCR”) provides the enforcement actions for violations of the Security Rule as well as the Data Breach Notification Rule and the Privacy Rule. Organizations covered by the rules (“covered entities”) are required to perform regular risk analysis, train all personnel and vendors, utilize physical safeguards for the e-PHI, and deploy technical measures such as encryption, multi-factor authentication, access controls, and other techniques to reduce the risk of data theft, loss, manipulation, or destruction.²⁶

The Security Rule enforces the protection of confidentiality that is at the heart of the HIPAA Privacy Rule. The Privacy Rule mandates confidentiality and limits the use of patient information. The Privacy Rule uses a very broad definition for PHI, covering all “individually identifiable health information” in any form or media, whether electronic, paper, or oral.²⁷ The PHI includes information and demographic data relating to

23. See 45 C.F.R. § 164.306(a) (2022). See also *Summary of the HIPAA Security Rule*, U.S. HEALTH AND HUM. SERVS., <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html> [https://perma.cc/5NTQ-4TGQ].

24. See, e.g., *What are the Penalties for HIPAA Violations?*, HIPAA J. (Jan 23, 2022), <https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/> [https://perma.cc/P75X-AF3B] (stating OCR . . . has the discretion to waive a financial penalty in the case of a data breach that could not be reasonably anticipated. “The penalty cannot be waived if the violation involved willful neglect of the Privacy, Security, and Breach Notification Rules.”).

25. *Summary of the HIPAA Security Rule*, *supra* note 23 (citing 45 C.F.R. § 164.306(a) (2022)).

26. See 45 C.F.R. § 164.306(a) (2022).

27. 45 C.F.R. § 160.103 (2022).

- the individual’s past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).²⁸

The Privacy Rule, Security Rule, and Data Breach Notification Rules create substantial obligations on the enterprises which host PHI regarding the protection of the data and the reporting requirements following any data incident that could expose PHI to unauthorized access or data theft.²⁹ In consequence, the reach of HIPAA is constrained to only a small subset of the medical infosystem. A “covered entity” under HIPAA includes a health plan, a health care clearinghouse, or a health care provider who transmits electronic health information in relation to a HIPAA-covered transaction.³⁰ It also includes another significant group of enterprises that operate as business associations of the covered entities. Business associates include a Health Information Organization, E-prescribing Gateway, or other person that “provides data transmission services with respect to protected health information to a covered entity,”³¹ those offering a personal health record to “one or more individuals on behalf of a covered entity,”³² and “any subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.”³³

Despite the challenges with the regulations, HIPAA remains the high-water mark for health care data protection. The OCR reports that “[s]ince the compliance date of the Privacy Rule in April 2003, OCR has received over 314,702 HIPAA complaints and has initiated over 1,148 compliance reviews.”³⁴ OCR has resolved 97 percent of the cases it has

28. See *Summary of HIPAA Privacy Rule*, *supra* note 19.

29. See Anupam Chander, Meaza Abraham, Sandeep Chandy, Yuan Fang, & Dayoung Park, *Achieving Privacy*, 74 SMU L. REV. 607, 637 (2021) (“DHHS . . . estimated that industry-wide implementation would cost \$3.2 billion in HIPAA’s first year and \$17.6 billion for the first ten years.”).

30. 45 C.F.R. § 160.103 (2022).

31. *Id.*

32. *Id.*

33. *Id.*

34. *Enforcement Results as of November 30, 2022*, U.S. HEALTH AND HUM. SERVS., (Dec. 19, 2022), <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html> [<https://perma.cc/4ASH-KAWB>].

investigated, imposing “a civil money penalty in 126 cases resulting in a total dollar amount of \$133,519,272.00.”³⁵ OCR enforcement is designed to force companies into better data privacy and security systems by making the cost of non-compliance too high to risk. At the same time, the consequence of falling victim to a ransomware attack of patient data theft then includes harms to the patients, disruption to the health provider, as well as a fine if the attack was due to a vulnerability in HIPAA compliance.

This vector of public health harm is likely being protected as best it can. Companies need to continue investing heavily in cybersecurity, but that need goes well beyond the health care sector alone. It is beyond the scope of this paper to address the structural issues that have given rise to the explosion of ransomware and cybertheft or how to address them at the national and global level.³⁶

B. *Personal Health Information Not Protected by HIPAA*

Between the covered entities and their business associates, the Privacy Rule and Security Rules reach a good deal of information collected by health care enterprises, but it excludes a great deal of additional information.³⁷ The pharmaceutical industry is not necessarily subject to HIPAA.³⁸ Nor are the multitude of health information websites and apps that are provided to the public outside of health care provider’s control. Health and wellness information offered through apps, websites, and social media have two discrete vectors for health care harms. First, they lack the protections of HIPAA related to the privacy and security of the information gathered. Second, they are often the source of

35. *Id.*

36. *See generally* STANISLAV ABAIMOV & MAURIZIO MARTELLINI, CYBER ARMS: SECURITY IN CYBERSPACE (2017); Amy Harrison Amy S. Harrison, Paul Sullivan, Alex Kubli, Kathleen M. Wilson Amy Taylor, Nicholas DeGregorio, Joseph Riggs, Maria Werner-Wasik, Adam Dicker, & Yevgeniy Vinogradskiy *How to Respond to a Ransomware Attack? One Radiation Oncology Department’s Response to a Cyber-Attack on Their Record and Verify System*, 12 PRAC. RADIATION ONCOLOGY 170 (2022), <https://www.sciencedirect.com/science/article/abs/pii/S1879850021002757> [<https://perma.cc/TY6G-BNCN>].

37. 20 U.S.C. §1232(g) (stating HIPAA, by statute, excludes employee health care information and student records under the Family Educational Rights and Privacy Act). *See also Summary of HIPAA Privacy Rule*, *supra* note 19.

38. *See* Nancy L. Perkins, *Marketing and Research: New HIPAA Privacy Rules Affect Pharmaceutical, Medical Device Companies’ Use of PHI*, BLOOMBERG L., (Mar. 8, 2013), <https://news.bloomberglaw.com/health-law-and-business/marketing-and-research-new-hipaa-privacy-rules-affect-pharmaceutical-medical-device-companies-use-of-phi> [<https://perma.cc/37TU-5GZH>] (“[P]harmaceutical companies very rarely are any of these types of entities.”).

misinformation and disinformation that shapes consumer behaviors and outcomes.

PHI not protected by HIPAA is subject to a patchwork of state laws that offer a combination of privacy requirements, security requirements, and data breach notification laws. “Five states—California, Colorado, Connecticut, Utah and Virginia—have enacted comprehensive consumer data privacy laws.”³⁹ Other states have a combination of requirements that companies post and adhere to a privacy policy along with a data breach notification requirement.⁴⁰ New York has created the leading model for a state analogy to the Security Rule with the enactment of the New York SHIELD Act.⁴¹ Massachusetts and Florida actually had two of the first such security obligations, although Florida only requires that companies provide “reasonable security measures.”⁴²

Complementing the patchwork of state laws, all companies are subject to the federal obligations of the Federal Trade Commission Act (“FTC Act”) not to engage in unfair and deceptive trade practices, under Section 5 of the FTC Act.⁴³ States have “baby FTC Acts” as well that are generally interpreted to following the interpretations of Section 5.⁴⁴ These

39. *State Laws Related to Digital Privacy*, NAT. CONF. OF STATE LEG., (June 7, 2022), <https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx> [<https://perma.cc/27MB-ZABM>]; *See also* California: CAL. CIV. CODE §§ 1798.100 *et seq.* (California Consumer Privacy Act of 2018 (CCPA) and California Consumer Privacy Rights Act (CPRA) Proposition 24, approved Nov. 2020, effective January 1, 2023); Colorado: COLO. REV. STAT. § 6-1-1301 *et seq.* (2021 S.B. 190); Connecticut: 2022 S.B. 6 (Personal Data Privacy and Online Monitoring); Utah: 2022 S.B. 227 (Utah Consumer Privacy Act); and Virginia: 2021 H.B. 2307/2021 S.B. 1392 (Consumer Data Protection Act).

40. Henry Adams, *The Federalist Regulation of Privacy: The Happy Incidents of State Regulatory Activity and Costs of Preemptive Federal Action*, 84 MO. L. REV. 1055, 1070 (2019) (“In an effort to address the increasingly common and harmful practice of unauthorized data access, California pioneered the first data breach notification regulation in 2002 by requiring that breached entities notify consumers in the event their personal information was compromised. By 2007, thirty-three states had enacted similar laws.”).

41. N.Y. GEN. BUS. LAW § 899-aa (McKinney 2019); N.Y. STATE TECH. LAW § 208 (McKinney 2019). *See* Eric B. Green, *The Gatekeepers of Research: Why A Data Protection Authority Holds the Key to Research in the New York Privacy Acts*, 87 BROOK. L. REV. 713, 748 (2022) (“On March 21, 2020, New York’s Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) went into effect.”).

42. 201 MASS. CODE REGS. 17.03–17.04 (2022); FLA. STAT. § 501.171 (2022). *See* Kimberly Dempsey Booher & Martin B. Robins, *American Privacy Law at the Dawn of A New Decade (and the CCPA and COVID-19): Overview and Practitioner Critique*, 24 MARQ. INTELL. PROP. L. REV. 169, 181 (2020).

43. 15 U.S.C. § 45 (2022).

44. CORP. COUNS. GUIDE TO UNFAIR COMPETITION § 10:1, INTRODUCTION, CORP. COUNS. GUIDE TO UNFAIR COMPETITION § 10:1 (2022) (“Many states have passed unfair competition laws called ‘baby FTC’ acts . . . with the distinction that the state acts generally provide for a private right of action and varying lists of specific misconduct constituting unfair or deceptive acts, or deceptive

general laws have been used by the FTC, and some state attorneys general, to enforce data security requirements and protect consumer data from unduly lax security protections.⁴⁵ Some of the state laws also provide a private right of action.⁴⁶

In addition, courts are increasingly recognizing that traditional notions of negligence require companies to take reasonable steps to protect the consumer information placed in those companies' care.⁴⁷ For example, in *In re Equifax, Inc. Customer Security Breach Litigation*,⁴⁸ the district court determined that "under traditional negligence principles, the Defendants owed a legal duty to the Plaintiffs to take reasonable precautions due to the reasonably foreseeable risk of danger of a data breach incident."⁴⁹

While there are a variety of state laws, common law liability, and federal regulations, these duties have not done a great deal to thwart the growing threats of cyberattacks and ransomware. Neither the motivation of the law enforcement nor the threats of harm from the cyberattacks are sufficient to end the scourge of cyberthreats.⁵⁰ "In 2021, the average number of cyberattacks and data breaches increased by 15.1% from the previous year."⁵¹ The 2022 report, *Cybersecurity Solutions for a Riskier World* by ThoughtLab,⁵² reports that "[t]he number of material breaches

practices and unfair methods of competition."); Carolyn Carter, *Consumer Protection in the United States, a 50-State Evaluation of Unfair and Deceptive Trade Practices*, NAT'L CONSUMER L. CTR. INC. (2018), https://www.nclc.org/wp-content/uploads/2022/09/UDAP_rpt.pdf [<https://perma.cc/JH2M-A9GX>].

45. See Danielle K. Citron, *Privacy Enforcement Pioneers: The Role of State Attorneys General in the Development of Privacy Law*, 92 NOTRE DAME L. REV. 747, 749 (2016) ("State attorneys general have been on the front lines of privacy enforcement since before the intervention of federal agencies.").

46. See, e.g., *Liu v. Amerco*, 677 F.3d 489, 491, 497 (1st Cir. 2012) (stating after the FTC brought a successful enforcement action against U-Haul under Section 5 of the FTC Act, Liu was permitted to bring suit under Mass. Gen. Laws ch. 93A, § 2(a), which permits private causes of action, based on the FTC's investigation and consent decree).

47. *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, CV 19-MD-2904, 2021 WL 5937742, at *14 (D.N.J. Dec. 16, 2021); *Brush v. Miami Beach Healthcare Grp. Ltd.*, 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017) ("It is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information.").

48. *In re Equifax, Inc. Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1321–27 (N.D. Ga. 2019).

49. *Id.*

50. See Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know*, FORBES (June 3, 2022), <https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/> [<https://perma.cc/RYA6-NK5M>].

51. *Id.*

52. *Cybersecurity Solutions for a Riskier World*, THOUGHTLAB, (Nov. 11, 2022), <https://thoughtlabgroup.com/cyber-solutions-riskier-world/> [<https://perma.cc/92SM-6T8T>].

respondents suffered rose 20.5% from 2020 to 2021.”⁵³ During the same time, the cost of increasingly insecure defense—as measured by a firm’s cybersecurity budget in comparison to its total revenue—“jumped 51%, from 0.53% to 0.80%.”⁵⁴ 2022 is tracking to be even worse. “Global attacks increased by 28% in the third quarter of 2022 compared to same period in 2021. The average weekly attacks per organization worldwide reached over 1,130 [attacks].”⁵⁵

“The main causes of these attacks [comes] from misconfigurations, human error, poor maintenance, and unknown assets.”⁵⁶ As computer systems become increasingly complex, the ability for the employees responsible for protecting these systems is becoming increasingly overwhelmed. Criminal misuse of stolen data and the opportunities to extort funds from firms using ransomware continue to make cybercrime highly lucrative. In addition, as a side effect of the Russian invasion of Ukraine, firms are potentially being targeted by Russia and Russian sympathizers to add disruptions and distractions to the ongoing international threat.⁵⁷ Given the inevitability of some degree of human error, the continually increasing complexity of networked computer systems, and incentives for bad actors to continue to launch cyberattacks, there is no reason to think that this trend will reverse itself in the next through years.

Thus, the first of the problems for health data outside of the HIPAA protected sphere is that there is less regulatory pressure to enforce stringent privacy and security protocols. Without the consequence of OCR fines, there is less investment on cybersecurity protections, less training

53. *Id.*

54. *Id.*

55. *Check Point Research: Third quarter of 2022 reveals increase in cyberattacks and unexpected developments in global trends*, CHECKPOINT, (Nov. 11, 2022), <https://blog.checkpoint.com/2022/10/26/third-quarter-of-2022-reveals-increase-in-cyberattacks/> [<https://perma.cc/B3A6-F674>].

56. Brooks, *supra* note 50.

57. *See generally Shields Up*, U.S. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, (Nov. 11, 2022), <https://www.cisa.gov/shields-up> [<https://perma.cc/S2KM-JTR5>] (“Evolving intelligence indicates that the Russian Government is exploring options for potential cyberattacks. Every organization—large and small—must be prepared to respond to disruptive cyber incidents.”); Mitchell Orenstein, *Russia’s Use of Cyberattacks: Lessons from the Second Ukraine War*, FOREIGN POL’Y RSCH. INST. (June 7, 2022), <https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks-lessons-from-the-second-ukraine-war/> [<https://perma.cc/3RSS-E5H3>] (“Russia uses cyberattacks as a method of disrupting societies and organizations. While in wartime, Russia deploys cyberattacks with greater frequency, and the attacks are often more destructive, the central difference appears to be the accompanying actions.”).

of staff, and slower responses to threats.⁵⁸ The lack of investment and focus reflects the security side of the problem. But outside of HIPAA, the privacy failures are even more problematic.

The FTC has recognized this issue in stark terms. Kristin Cohen, Acting Associate Director for the FTC Division of Privacy & Identity Protection explained the problem:

Among the most sensitive categories of data collected by connected devices are a person's precise location and information about their health. Smartphones, connected cars, wearable fitness trackers, "smart home" products, and even the browser you're reading this on are capable of directly observing or deriving sensitive information about users. Standing alone, these data points may pose an incalculable risk to personal privacy. Now consider the unprecedented intrusion when these connected devices and technology companies collect that data, combine it, and sell or monetize it. . . .

Beyond location information generated automatically by consumers' connected devices, millions of people also actively generate their own sensitive data, including by using apps to test their blood sugar, record their sleep patterns, monitor their blood pressure, or track their fitness, or sharing face and other biometric information to use app or device features. The potent combination of location data and user-generated health data creates a new frontier of potential harms to consumers.⁵⁹

But despite its protestations, the FTC has done little to protect against these threats. The same column regarding the protection of the public's health information identified only four actions undertaken by the FTC

58. See, e.g., Bharath Aiyer, Jeffrey Caso, Peter Russell & Marc Sorel, *New survey reveals \$2 trillion market opportunity for cybersecurity technology and service providers*, MCKINSEY & CO. (Oct. 27, 2022), <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers> [https://perma.cc/9K2B-6ZS6] ("In the face of this cyber onslaught, organizations around the world spent around \$150 billion in 2021 on cybersecurity, growing by 12.4 percent annually. However, set against the scale of the problem, even this 'security awakening' is probably insufficient."); Arti Loftus, *Massive Fines in Travel and Hospitality Illustrate Investments in Cyber Security Are Risk Management Strategies*, TECHZONE360 (July 12, 2019), ("Network security continues to be an afterthought for a large percentage of companies," said Ed Wood, CEO, Dispersive. . . . "This is indicated by the 43% of companies that are looking at the next three years to address their cybersecurity needs. There needs to be a sense of more urgency.").

59. Kristin Cohen, *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, FTC BUSINESS BLOG (July 11, 2022), <https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal> [https://perma.cc/SL2Y-URLZ].

involving such data misuse along with one example of a settlement brought by the Massachusetts Attorney General.⁶⁰

One of the FTC actions illustrates the extent to which non-regulated companies take advantage of the public.

Flo Health pitched its Flo Period & Ovulation Tracker as a way for millions of women to “take full control of [their] health.” But according to the FTC, despite express privacy claims, the company took control of users’ sensitive fertility data and shared it with third parties – a broken promise that left consumers feeling “outraged,” “victimized,” and “violated.”⁶¹

In violation of the posted terms of service and legal restrictions, Flo provided health information including pregnancy status to third parties.⁶²

In a 2014 report, the FTC noted that data brokers collect and combine information to create personalized profiles, including health and health-related information.⁶³ The report identified that “potentially sensitive categories highlight certain health-related topics or conditions, such as ‘Expectant Parent,’ ‘Diabetes Interest,’ and ‘Cholesterol Focus.’”⁶⁴ Using these tools, data brokers and their clients use credit-like, undisclosed

60. *Id.* (citing a Massachusetts settlement with Copley Advertising, LLC (Copley)); see *AG Reaches Settlement with Advertising Company Prohibiting ‘Geofencing’ Around Massachusetts Healthcare Facilities*, PRESS RELEASE OFF. OF ATT’Y GEN. MAURA HEALEY (Apr. 4, 2017), <https://www.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts-healthcare-facilities> [<https://perma.cc/9UJS-VNBL>].

61. Lesley Fair, *Health app broke its privacy promises by disclosing intimate details about users*, FED. TRADE COMM’N BUS. BLOG (Jan. 13, 2021), <https://www.ftc.gov/business-guidance/blog/2021/01/health-app-broke-its-privacy-promises-disclosing-intimate-details-about-users> [<https://perma.cc/PW8Y-LZNG>]. See Complaint at 4, In the Matter of Flo Health, Inc., No. 1923233, (FTC 2020), https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf [<https://perma.cc/K2JQ-MXHX>].

[B]eginning in 2016, Respondent handed users’ health information out to numerous third parties, including Google, LLC (“Google”); Google’s separate marketing service, Fabric (“Fabric”); Facebook, Inc., through its Facebook Analytics tool (“Facebook”); marketing firm AppsFlyer, Inc. (“AppsFlyer”); and analytics firm Flurry, Inc. (“Flurry”). And Respondent took no action to limit what these companies could do with the users’ information. Rather, they merely agreed to each company’s standard terms of service. By doing so, Respondent gave these third parties the ability to use Flo App users’ personal health information expansively, including for advertising.

62. Fair, *supra* note 61.

63. Julie Brill, Terrell McSweeney, Maureen Ohlhausen, Edith Ramirez & Joshua Wright, *Data Brokers: A Call for Transparency and Accountability*, FTC (May 2014), <https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014> [<https://perma.cc/Z4P9-BPHK>].

64. *Id.* at 47.

scores for providing various goods and services to the public.⁶⁵ These scores can result in disparate impacts based on race, gender, or other biases inherent in the profiling models.

The risks that consumer scores can pose include potential bias and adverse effects, and the scores generally lack transparency. The data used to create scores may contain racial biases—for example, one study found Black patients were assigned lower risk scores than White patients with the same health care needs, predicting less of a need for a care management program.⁶⁶

Other uses of the profiles allow health care providers to screen for patients and clients.⁶⁷ In addition to the questionable legality of using these scores to determine health care access, the nature of the data used is itself suspect. The data brokers rely heavily on publicly available data that is not evaluated for its accuracy.⁶⁸ Disclaimers and “as is” provisions in the data contracts do little to protect the individual from the loss of services caused by inaccuracies in the data sets purchased or scraped to feed the scoring models.

The information collected about an individual’s health care status, concerns, and behaviors can be used for much more than advertising and scoring. While the use of such data for job discrimination and insurance discrimination are often concerns, the recent changes to abortion access has turned this information into potential criminal evidence.⁶⁹ “In the first

65. *See id.* at 36. *See also Congress Should Consider Enhancing Protections around Scores Used to Rank Consumers*, U.S. GOV’T ACCOUNTABILITY OFF. (May 2022), <https://www.gao.gov/assets/gao-22-104527.pdf> [<https://perma.cc/HG97-SZMB>] [hereinafter *GAO Report*].

66. Brill, *supra* note 65.

67. *Id.* at 8. ([A data broker] “offers a collection score that assists hospitals with grouping patients based on their likelihood of not making a payment, which could help users identify how much a patient could be expected to pay and which cases would need to be outsourced to collection agencies.”). *See also* Zaid Obermeyer, Brian Powers, Christine Vogeli & Sendhil Mullainathan, *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 *SCIENCE* 447 (2019).

68. *GAO Report*, *supra* note 65, at 18.

One leading score creator—which produces scores used in insurance, fraud prevention, identity verification, health care, and more—states on several of its scoring product web pages or product brochures that the public records and commercially available data sources underlying several of its products may contain errors due to inaccurate reporting, data entry, or processing.

69. *See* Bobby Allyn, *Privacy advocates fear Google will be used to prosecute abortion seekers*, NAT. PUB. RADIO (July 11, 2022), <https://www.npr.org/2022/07/11/1110391316/google-data-abortion-prosecutions> [<https://perma.cc/P7ER-8NNY>] (“[O]ften, finding out where someone was at the time of a crime, or what they were Googling before a crime occurs, can be pivotal to investigators. Now . . . privacy advocates fear Google will provide users’ data to authorities who may try to target people seeking abortions.”).

half of [2021], law enforcement sent Google more than 50,000 subpoenas, search warrants and other types of legal requests for data Google retains.”⁷⁰

Google, Facebook, and other advertising-based enterprises acquire data from a seemingly infinite number of sources, which, in turn, makes these companies one-stop-shops for law enforcement and others interested in tracking individuals or populations. Among the most concerning of these partnerships, is the agreement between PlanCPills.org with both Facebook and Google to provide user data.⁷¹ “According to Johnny Lin, founder of the tracker blocking app Lockdown Privacy, Plan C’s site contains trackers that transmit information to Facebook and Google, including visitors’ IP addresses, the URLs they’re browsing — which can contain the state in which they’re seeking abortions — and unique identifiers. . . .”⁷² Whether the information is used to sell advertisements for health care products or right to life messages, the use of such personal information is not likely what the users of PlanCPills.org expect to be included in its privacy notice. It certainly seems out of character for a service designed to keep abortion access legal, rather than more easily prosecuted.

While abortion is a hot-topic political issue, the same concerns apply to drug and alcohol treatments, sexually transmitted disease information, mental health services, or any other form of health care for whom the party seeking treatment might also have concerns about the information being used adversely in the workplace or social settings. As the PlanC example illustrates, even the most sensitive of health care data is simply part of the commercial trade in the public’s private lives.

C. *The Exacerbating Threat of Misinformation and Disinformation*

If the picture of health information data security were not bleak enough, that is only one of the twin threats to the health infosystem. The second major threat comes from misinformation and disinformation⁷³ in

70. *Id.*

71. Issie Lapowsky, *Plan C is a top abortion pill resource. It’s also sharing data with Facebook and Google*, PROTOCOL (July 12, 2022), <https://www.protocol.com/policy/plan-c-trackers> [<https://perma.cc/WW3B-D4A9>].

72. *Id.*

73. See ANAHI AYALA IACUCCI, UNHCR INNOVATION, USING SOCIAL MEDIA IN COMMUNITY-BASED PROTECTION: A GUIDE, UNITED NATIONS HUMAN RIGHTS COUNCIL 16 (Helen Womack ed., January 2021) [hereinafter UNHCR] (“Misinformation is information that is false but not created with the intention of causing harm. It differs from Disinformation, which is false and deliberately created to harm a person, social group, organization or country. . . .”).

the massive marketplace for health and wellness information and communications.

Health disinformation affects both individuals and vulnerable communities.

One of the most successful early Soviet disinformation campaigns, Operation Infektion, took place in the 1980s. The heart of Operation Infektion was the lie that HIV was invented by the United States government as a tool of genocide against its African American and gay citizens. KGB agents planted this rumor in a single article published in a small newspaper in New Delhi, India. They then wrote additional articles first in African media, later in the *Moscow Times*, citing the New Delhi article. They paid a scientist from East Germany to corroborate the “science” of behind the claim. The story finally hit US nightly news screens three years later. The rumor swept through African American communities, generating enough public commentary and concern that the then leader of the USSR, Gorbachev, apologized publicly to President Reagan the following year. However, the false rumor proved durable. As recently as 2005, a survey of 500 randomly selected African Americans found that 48% believed HIV was a manmade virus and 16% thought the government created AIDS to control the black population.⁷⁴

This chilling reminder that entire populations may be sacrificed to create pawns in a geopolitical game is not merely historical. Publishing this article on weaponizing health care data, researchers at the Harvard Kennedy School’s Belfer Center for Science and International Affairs noted a Russian-backed effort to amplify the anti-vaccine movement.

In 2018, Russia undertook an extensive social media-mediated disinformation campaign to amplify the anti-vaccination movement. Researchers have confirmed that Russian trolls and bots tweeted anti-vaccination messages at twice to twelve times the rate of average users and Twitter users were twenty-two times more likely to come into contact with anti-vaccination messages. Furthermore, research shows exposure to these messages significantly decreases vaccine uptake.

74. Margaret Bourdeaux, Gbemisola Abiola, Ben Edgar, James Pershing, Joyce Wang, Margot Van Loon & Bruce Schneier, *Weaponizing Digital Health Intelligence*, BELFER CTR. FOR SCI. & INT’L AFF., HARV. KENNEDY SCH. (Jan. 2020), <https://www.belfercenter.org/publication/weaponizing-digital-health-intelligence> [<https://perma.cc/X342-T8PA>] (citing Adam B. Ellick & Adam Westbrook, *Opinion Video Series: Operation Infektion: Russian Disinformation: From Cold War to Kanye*, N.Y. TIMES. (Nov. 12, 2018) <https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html> [<https://perma.cc/MV9W-E75Z>]; Laura M. Bogart & Sheryl Thorburn, *Are HIV/AIDS Conspiracy Beliefs a Barrier to HIV Prevention Among African Americans?*, 38 J ACQUIR IMMUNE DEFIC SYNDR 213, 213–18 (2005)).

People who choose not to vaccinate their children report their main sources of media and news are social media platforms such as Facebook and Twitter.⁷⁵

The impact of this Russian disinformation campaign has been traced back earlier to part of the 2014 interference with the U.S. elections and extended into the response to the COVID-19 vaccines.⁷⁶ As a consequence, health care disinformation, just like cyberattacks, can originate with belligerent nations in addition to criminal actors and hacktivists.⁷⁷

Health and wellness content is distributed by a combination of books and magazines, television and video, websites, apps, and social media services.⁷⁸ Such information dominates nonfiction media, is fully protected by the First Amendment, and is rife with risks to the nation's health. The self-help publishing field is quite popular and profitable. "NPD Group reports that the self-help industry has grown rapidly in recent years: from 2013 to 2019, self-help book sales in the United States increased by 11 percent, reaching 18.6 million volumes. Over the same time period, the number of self-help titles nearly doubled, rising from 30,897 to 85,253."⁷⁹ No published data differentiates publications on general well-being information from those on mental health or medical information. But even if these books reflect only a small portion of the 85,000 titles, the industry has grown quite robust.

75. Bourdeaux et al., *supra* note 74 (citing David A. Broniatowski, Amelia M. Jamison, SiHua Qi, Lulwah AlKulaib, Tao Chen, Adrian Benton, Sandra C. Quinn & Mark Dredze, *Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate*, 108 *AJPH* 1378 (2018)).

76. Peter J. Hotez, *Anti-science kills: From Soviet Embrace of Pseudoscience to Accelerated Attacks on US Biomedicine*, 19 *PLOS BIOL.* Jan. 28, 2021, at 1, 4 ("Today, Russian politicization of biomedicine—the biological sciences as they apply to translational medicine—reveals a confusing or ambivalent system of legitimate scientific endeavors alternating with an ever-widening program of disinformation designed to undermine the field. This is especially true in the area of vaccines.").

77. See C. Todd Lopez, *In Cyber, Differentiating Between State Actors, Criminals Is a Blur*, DEPT. OF DEFENSE NEWS (May 14, 2021), <https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur/> [<https://perma.cc/4V6H-E7QV>]; KEVVIE FOWLER, DATA BREACH PREPARATION AND RESPONSE 9 (Curtis Rose, ed.) (2016) ("Hacktivists are groups of criminals who unite to carry out cyber attacks in support of political causes. Hacktivists typically target entire industries but sometimes attack specific organizations who they feel don't align with their political views or practices.").

78. See generally Israel Júnior Borges do Nascimento, Ana Beatriz Pizarro, Jussara M Almeida, Natasha Azzopardi-Muscat, Marcos André Gonçalves, Maria Björklund & David Novillo-Ortiz, *Infodemics and Health Misinformation: A Systematic Review of Reviews*, 100 *BULL WORLD HEALTH ORG.* 544 (2022).

79. Bobby Mollison, *The History of Self-Help Books*, TAGARI PUBL'NS (Feb. 9, 2022), <https://www.tagari.com/how-many-self-help-books-have-been-published/> [<https://perma.cc/6NPR-PJ3S>].

The television market is increasingly interconnected to the social media market, but both singly and together, these do not provide effective health information. A study by Penn State suggests that that “[p]eople who relied on TV news and social media were less knowledgeable about COVID-19 than other people during the early days of the pandemic.”⁸⁰ Television was not an effective educational source for pandemic information.⁸¹ Other studies highlight that COVID-19 information was closely tied to the correlated political leanings of the associated news source, such as, either Fox or MSNBC.⁸² Social media sources, such as Facebook, were not significantly more accurate than television.⁸³ While the empirical data are subject to many sample caveats, the implications are significant. “This is concerning, as half of Americans report using television as a source of news and 66% of Americans use social media such as Facebook as a news source.”⁸⁴

YouTube does not fare better. YouTube has become a dominant streaming media and social media hybrid content outlet. YouTube has powerful reach. “[O]ver 95% of the Internet population are regularly interacting with YouTube in 76 different languages from more than 88 countries. A telephone survey conducted in the United States revealed that more than 74% of adults were using YouTube in September 2020.”⁸⁵ A recent medical study on YouTube reported flatly, “YouTube is not a

80. Robby Berman, *TV News was the Main Source of Early COVID-19 Misinformation for Some in the US*, MED. NEWS TODAY (April 15, 2021), <https://www.medicalnewstoday.com/articles/tv-news-was-the-main-source-of-early-covid-19-misinformation-for-some-in-the-us> [https://perma.cc/X6RU-4A6Z] (discussing Surav Man Sakya, Lauren Jodi Van Scoy, John C. Garman, Erin L. Miller, Bethany Snyder, Emily Wasserman, Vernon M. Chinchilli & Robert P. Lennon *The Impact of COVID-19-Related Changes in Media Consumption on Public Knowledge: Results of a Cross-Sectional Survey of Pennsylvania Adults*, 37 CURRENT MED. RSCH. & OP., Apr. 11, 2021, at 911).

81. Sakya et al., *supra* note 80, at 914 (“Those who relied on television news as a primary source, or who used Facebook as an additional news source generally, were less likely to answer COVID-19 questions correctly than other groups.”).

82. Mark Jurkowitz & Amy Mitchell, *Cable TV and COVID-19: How Americans Perceive the Outbreak and View Media Coverage Differ by Main News Source*, PEW RSCH. CTR. (Apr. 1, 2020), <https://www.pewresearch.org/journalism/2020/04/01/cable-tv-and-covid-19-how-americans-perceive-the-outbreak-and-view-media-coverage-differ-by-main-news-source/> [https://perma.cc/Y6JY-L9WF] (“[T]he responses to COVID-19 news from those whose main source for political news is MSNBC or Fox News are strikingly different. The views of those who identify CNN as their main news source most often fit somewhere between the two.”).

83. *See* Sakya et al., *supra* note 80, at 914.

84. *Id.*

85. Wael Osman, Fatma Mohamed, Mohamed Elhassan & Abdulhadi Shoufan, *Is YouTube a Reliable Source of Health-Related Information? A Systematic Review*, 22 BMC MED. EDUC. 1, 1–2 (2022) (internal citations omitted).

reliable source of medical and health-related information.”⁸⁶ The majority of videos (54%) were reported to reflect a commercial bias of the video publisher.⁸⁷ A mere 32% of the videos provided health information in an objective, neutral manner.⁸⁸ And there was no correlation between the quality of the health information and the popularity of the video in terms of views or likes, so that the social promotion of health content was completely unrelated to the quality of the content available.⁸⁹ In other words, the actual marketplace for ideas fails to promote accurate or unbiased ideas over those that are commercially motivated or publicly popular. The open marketplace fails to promote truthful information.

The other content marketplace is even more problematic. This is the smartphone app marketplace. A survey conducted in 2017 reports that 325,000 mobile health apps were featured on Google’s Android and Apple’s iOS platforms.⁹⁰ Although HIPAA-regulated health care providers increasingly use web and app interfaces to share information with patients, the vast majority of these apps are written by third parties. The health app environment appears to be particularly ripe for misinformation and disinformation.

The proliferation of mobile health apps has largely been without oversight or regulation, and the quality of these apps is highly variable. For example, smoking cessation apps were found to rarely adhere to established medical guidelines[.]. In addition, while 95% of cancer information apps aimed at health care workers contained scientifically valid information, this was true of only 32% of apps aimed at the general public[.].⁹¹

In addition to the proliferation of health and wellness apps, the National Institute on Aging notes that “[t]here are thousands of medical websites. Some provide reliable health information. Some do not.”⁹² In 2019, the year before COVID-19 health information was politicized and

86. *Id.* at 10.

87. *Id.* at 7.

88. *Id.*

89. *Id.*

90. Markus Pohl, *325,000 Mobile Health Apps Available in 2017 – Android Now the Leading mHealth Platform*, RESEARCH2GUIDANCE, <https://research2guidance.com/325000-mobile-health-apps-available-in-2017/> [<https://perma.cc/5LUQ-TGAU>] (last visited Oct. 12, 2022) (Android had 158,000 apps according to the data while iOS has approximately 150,000. Since most vendors offer the same service on both platforms, it is likely that many apps appear on both platforms.).

91. Swire-Thompson & Lazer, *supra* note 9, at 437.

92. Nat’l Inst. on Aging, *How To Find Reliable Health Information Online*, NAT’L INSTS. OF HEALTH, <https://www.nia.nih.gov/health/online-health-information-it-reliable> [<https://perma.cc/P2S2-B7YF>] (last visited Nov. 10, 2022).

weaponized, the information-rating service NewsGuard⁹³ looked into the veracity of health information websites after false information began to spread regarding a measles outbreak. “Of the sites analyzed by NewsGuard, 11% provide misinformation about health...”⁹⁴ While a misinformation rate of 11% seems rather modest, their reach was not. “These sites accounted for more than 49 million engagements (shares, likes, comments, etc.) on social media in the past 90 days—more than major news websites such as NPR, Business Insider, or Forbes.”⁹⁵

Apps, websites, and social media outlets are just a few of the sources of health care misinformation. “Misinformation and disinformation are introduced online by many different sources: vested interests, politicians[], news media[], gossip, and works of fiction[.]”⁹⁶ Disinformation is distinct from mere misinformation because “disinformation incorporates the notion of intentionality.”⁹⁷ “Disinformation is a coordinated or deliberate effort to knowingly circulate misinformation in order to gain money, power, or reputation.”⁹⁸

Disinformation is not limited to any one media platform. “Contemporary models of contagion and epidemiological studies of misinformation suggest that false information diffuses faster and farther than true information, particularly in the context of social media.”⁹⁹ These phenomena continue to grow in scope. The jump from measles disinformation in 2019 to COVID-19 disinformation in 2020 was a natural progression. “For example, one recent study found over 2000 COVID-19 related rumors, stigma, and conspiracy theories in 25 languages from 87 countries. The authors concluded that of these reports, 82% of them were false, highlighting the need for interventions aimed to combat

93. *Our Team*, NEWSGUARD, <https://www.newsguardtech.com/about/team/> [https://perma.cc/AJB7-Q9TC] (“Co-CEOs . . . Steven Brill and Gordon Crovitz are veteran journalists and news entrepreneurs. Brill founded The American Lawyer, Court TV, and the Yale Journalism Initiative. Crovitz was publisher of The Wall Street Journal and a columnist for the paper. Together, they have supervised thousands of journalists around the world.”).

94. John Gregory, *Health Websites are Notoriously Misleading. So We Rated Their Reliability*, STAT (July 26, 2019), <https://www.statnews.com/2019/07/26/health-websites-are-notoriously-misleading-so-we-rated-their-reliability/> [https://perma.cc/RCB3-HNKM].

95. *Id.*

96. Swire-Thompson & Lazer, *supra* note 9, at 437.

97. *Id.* at 435.

98. *Id.* See also UNHCR, *supra* note 73, at 230 (“Misinformation is false or inaccurate information. Examples include rumors, insults and pranks. Disinformation is deliberate and includes malicious content such as hoaxes, spear phishing and propaganda. It spreads fear and suspicion among the population.”).

99. Angel N. Desai, Diandra Ruidera, Julie M. Steinbrink, Bruno Granwehr & Dong Heun Lee, *Misinformation and Disinformation: The Potential Disadvantages of Social Media in Infectious Disease and How to Combat Them*, 74 CLINICAL INFECTIOUS DISEASES e34 (2022).

misinformation.”¹⁰⁰ These false claims are fueled by other users, by “trolls” seeking to disrupt the platform, and by automated software designed to mirror actual user activity. “One early study of Twitter concluded that approximately 53% of initial users were human; the rest were classified as cyborgs or bots, which are automated accounts on social media platforms created to imitate human activity.”¹⁰¹

Social media disinformation is coupled with another phenomenon fairly unique to the modality, that of attacking and trolling those who seek to provide accurate health information.¹⁰² In a 2020 study, 91.9% of prominent scientists, clinicians and patient advocates “experienced abusive behavior, including persistent harassment (69.3%) and physical violence and intimidation (5.9%). A substantial number (38.6%) received vexatious complaints to their employers, professional bodies or legal intimidation.”¹⁰³ Such trolling and other harmful behavior creates an asymmetric risk that suggests a marketplace of ideas fails when those seeking to promote self-interested and harmful information are also willing to harass and abuse those seeking to add accurate, objective health information of half of the public.

A recent report highlights the problem. In fall 2022, the Wall Street Journal illustrates the increasingly common practice.¹⁰⁴

In a four-week period spanning October and November [2022], about 20 companies ran more than 2,100 ads on Facebook and Instagram that described benefits of prescription drugs without citing risks, promoted drugs for unapproved uses or featured testimonials without disclosing whether they came from actors or company employees, according to a Wall Street Journal analysis of ads collected by the nonprofit

100. *Id.* (citing Md Saiful Islam, Tonmoy Sarkar, Sazzad Hossain Khan, Abu-Hena Mostofa Kamal, S. M. Murshid Hasan, Alamgir Kabir, Dalia Yeasmin, Mohammad Ariful Islam, Kamal Ibne Amin Chowdhury, Kazi Selim Anwar, Abrar Ahman Chughtai & Holly Seale, *COVID-19–Related Infodemic and Its Impact on Public Health: A Global Social Media Analysis*, 103(4) AM. J. TROPICAL MED. & HYGIENE 1621, 1621–29 (2020)).

101. Desai, *supra* note 99 (citing Zi Chu, Steven Gianvecchio, Haining Wang & Sushil Jajodia, *Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?*, 9 IEEE TRANSACTIONS ON DEPENDABLE & SECURE COMPUTING, no. 6, 2012, at 811, 824).

102. See David R. Grimes, Laura J. Brennan & Robert O’Connor, *Establishing a Taxonomy of Potential Hazards Associated with Communicating Medical Science in the Age of Disinformation*, 10 BMJ OPEN, July 5, 2020, at 1.

103. *Id.* at 1–2. (In the study, prominent medical science communicators was “defined as having >1000 Twitter followers and experience communicating medical science on social and traditional media platforms.”).

104. See Khadeeja Safdar & Andrea Fuller, *Misleading Ads Fueled Rapid Growth of Online Mental Health Companies*, THE WALL ST. J. (Dec. 27, 2022 12:14 pm ET), <https://www.wsj.com/articles/telehealth-cerebral-done-ads-mental-health-adhd-11672161087> [<https://perma.cc/5APW-4BBN>].

Algorithmic Transparency Institute from Meta Platforms Inc.’s ad library.

Those drugs included controlled substances, such as ketamine and testosterone, which are tightly regulated by the federal government due to their potential for abuse, and medications that normally carry boxed warnings, among the most serious types of safety warnings mandated by the FDA.¹⁰⁵

Individuals struggling with mental health issues or other medical problems are particularly vulnerable to this trolling behavior in which they are enticed by over and over, often through ads produced to look very much like user content, into trusting these actors pretending to be real people helped by these medications. “Digital ad spending by telehealth companies swelled to more than \$100 million in 2021 from around \$10 million in 2020, according to an analysis of ad spending by 18 telehealth startups conducted by Pathmatics, a marketing research firm.”¹⁰⁶ While these numbers do not compare to the spending in other sectors, they indicate a significant increase caused by yet another lapse in the regulatory scheme. In addition, “[t]he tally doesn’t include TikTok, which collected more than \$23 million from these telehealth advertisers this year through November.”¹⁰⁷

III. INDIVIDUAL AUTONOMY IN HEALTH CARE AND HEALTH INFORMATION VERSUS THE THREATS OF SLUDGE AND DARK PATTERNS.

One of the key concerns regarding governmental control over health information protection is the extent to which individual members of the public have the right to explore health and wellness strategies that are not governmentally approved. For some, government protection equates to governmental control. Many believe the health benefits of marijuana are substantially superior to that of the federal government¹⁰⁸ and others feel

105. *Id.* In an unrelated report, one of the drugs promoted on Facebook and Instagram, ketamine, was recently linked to schizophrenia-like symptoms. See HSE Univ.-Perm, *Ketamine’s Schizophrenic-Like Effects Could Aid Psychosis Research*, SCIENCEBLOG (Dec. 31, 2022), <https://scienceblog.com/535703/ketamines-schizophrenic-like-effects-could-aid-psychosis-research/> [<https://perma.cc/K5AC-X5M4>] (“The drug ketamine can cause brain changes similar to those found in people with schizophrenia. When taken by healthy people, ketamine can cause hallucinations and delusions, common in schizophrenia.”).

106. Safdar, *supra* note 104.

107. *Id.*

108. Nat’l Ctr. For Complementary & Integrative Health, *Compare Cannabis (Marijuana) and Cannabinoids: What You Need To Know*, NAT. INST. HEALTH (Nov. 2019) <https://www.nccih.nih.gov/health/cannabis-marijuana-and-cannabinoids-what-you-need-to-know> [<https://perma.cc/629T-KRAW>] with NAT’L ACAD. OF SCI., *THE HEALTH EFFECTS OF CANNABIS AND*

the same way regarding psychedelic mushrooms.¹⁰⁹ Approved practices, such as thalidomide for morning sickness, have proven to be medically disastrous.¹¹⁰ The fighting faiths of medical dogma are often proven unreliable, and all science is subject to constant correction and amendment.¹¹¹ As a consequence, there is a critical role in the health care and public health arena for individual choice. Moreover, beyond the mere risk of inaccuracies by government health officials and established medical practices, there is an important role in individual autonomy in making personal medical decisions—even if they are wrong and perhaps self-harming.

This balance, between the individual and the state, has been at the heart of all regulation. As an initial question, one must ask whether this matters at all. Autonomous rationality, as embodied in the notion of *homo economicus* or the rational person,¹¹² postulates that individuals are driven by rational economic choices to promote “accumulation, leisure, luxury and procreation.”¹¹³ The economic model underlying this school of thought presumed that choice was rational and directive. Health choices, one would postulate under this model, would be a rationally based choice.¹¹⁴

CANNABINOIDS: THE CURRENT STATE OF EVIDENCE AND RECOMMENDATIONS FOR RESEARCH (2017), <https://www.ncbi.nlm.nih.gov/books/NBK425767/> [<https://perma.cc/E8VB-SFJU>].

109. See, e.g., Henry Lowe, Ngeh Toyang, Blair Steele, Henkel Valentine, Justin Grant, Amza Ali, Wilfred Ngwa & Lorenzo Gordon, *The Therapeutic Potential of Psilocybin*, 26 MOLECULES, May 15, 2021, at 2948.

110. See James H. Kim & Anthony R. Scialli, *Thalidomide: The Tragedy of Birth Defects and the Effective Treatment of Disease*, 122 TOXICOLOGICAL SCI. 1 (2011).

111. See Naomi Oreskes, *If You Say ‘Science Is Right,’ You’re Wrong*, SCI. AM. (July 1, 2021), <https://www.scientificamerican.com/article/if-you-say-science-is-right-youre-wrong/> [<https://perma.cc/KG7Y-RCA2>] (“Science is a process of learning and discovery, and sometimes we learn that what we thought was right is wrong. Science can also be understood as an institution (or better, a set of institutions) that facilitates this work.”).

112. See Joseph Persky, *Retrospectives: The Ethology of Homo Economicus*, 9 J. ECON. PERS. 221 (1995) (While John Stuart Mill is generally identified as the creator of economic man, he never actually used this designation in his own writings. But the term did emerge in reaction to Mill’s work.). See generally Efe Efeoğlu & Yurdanur Çalışkan, *A Brief History of Homo Economicus From The Economics Discipline Perspective*, ATU J. SOC. SCI. (Feb. 28, 2019); Philipp Schreck, Dominik van Aaken, & Karl Homann, “There’s Life in the Old Dog Yet”: *The Homo Economicus Model and its Value for Behavioral Ethics*, 90 J. BUS. ECON. 401 (Nov. 19, 2019).

113. Persky, *supra* note 112, at 223. See also Efeoğlu & Çalışkan, *supra* note 112, at 31 (Mill equated aversion to pain as the same phenomenon as desire for pleasure. “Mill (1861) says, ‘Desiring a thing and finding it pleasant, aversion to it and thinking of it as painful are phenomena entirely inseparable, rather two parts of the same phenomena.’”) (quoting JOHN STUART MILLS, UTILITARIANISM (Parker, Son, and Bourn 1863)).

114. Douglas E. Hough, *Irrationality in Health Care*, HEALTH POL’Y 8, 8 (Dec. 2016), https://www.ispor.org/docs/default-source/publications/value-outcomes-spotlight/november-december-2016/vos-irrationality-in-health-care.pdf?sfvrsn=1efa4b23_2 [<https://perma.cc/U2FP->

Adam Smith added to this paradigm in the economic setting. In Adam Smith's 1776 economic opus, "The Wealth of Nations," Smith captures the rational economic self-interest that aligns with the greater good. He wrote "it is not from the benevolence of the butcher, the brewer, or the baker, that we expect our dinner but from their regard to their own interest. We address ourselves, not to their humanity but their self-love, and never talk to them of our own necessities but of their advantages."¹¹⁵ When combined with Adam Smith's benign explanation of self-interest, it framed a clear expectation that economic models were rational and driven by the enlightened self-interest of the people who comprised a market.

Mill's homo economicus and Smith's hidden hand of the marketplace find traction in the early development of the First Amendment. The rational and self-correcting nature of this libertarian ideal was defended in Mill's 1859 publication, "On Liberty," where he argued against any restriction on the press as a protection against a corrupt state, and, more generally, against the state's interest in suppressing "false opinion," since "We can never be sure that the opinion we are endeavouring to stifle is a false opinion; and if we were sure, stifling it would be an evil still."¹¹⁶

Supreme Court Justice Oliver Wendell Holmes endorsed this operationalist view into the constitutional framework with his famous dissent in *Abrams v. United States*,¹¹⁷ where he echoed Mill by writing:

But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas — that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and

65N5] (Pertaining to individual choice, "[i]f people do not know what is going to make them better off or give them pleasure, then the idea that you can trust people to do what will give them pleasure becomes questionable." (quoting Nobel Prize winner Daniel Kahneman)); Deirdre McCaughey & Nealia S. Bruning, *Rationality Versus Reality: The Challenges of Evidence-Based Decision Making for Health Policy Makers*, 5 IMPLEMENTATION SCI., NO. 39, 2010, at 1 (discussing the rationality of public health decisions by policy makers).

115. ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS Vol. 1, 17 (1776). See Efeoğlu & Çalışkan, *supra* note 112, at 30 ("The economic behavior of Man in commercial society would be based on straightforward self-interest plus instrumental rationality. It is also significant in this context that self-love and self-interest are used interchangeably by Smith.").

116. JOHN STUART MILL, ON LIBERTY 84 (1859).

117. *Abrams v. United States*, 250 U.S. 616 (1919).

that truth is the only ground upon which their wishes safely can be carried out.¹¹⁸

This dissent by Holmes, of course, carried the day.¹¹⁹

Although economics and social science have come far from the model espoused by Mill, Adams, and Holmes, the constitutional First Amendment jurisprudence has not. Instead, it holds these truths to be self-evident. Particularly in the highly inconsistent area of commercial speech, the Mill-Holmes model of rationality and philosophical marketplace has become an abstract prophylactic to justify jurisprudential interference with democratic regulation. Nowhere is that harm more evident than in the health care field.

A robust body of scientific literature has emerged in the late twentieth century postulating that homo sapiens are not the rational beings conceived in the economics of homo economicus. Although the Old Testament may have been trying to teach us this lesson since the story of Adam and Eve or Cain and Abel,¹²⁰ behavioral economics actually can ascribe this economic truth again to Adam Smith. Prior to *Wealth of Nations*, Smith focused on individual behavior. He “asserted we are all endowed with moral sentiments, which ultimately drive our behaviour. . . . Smith wrote about the absolute importance of

118. *Id.* at 630 (Holmes, J., dissenting).

119. *See* *Brandenburg v. Ohio*, 395 U.S. 444, 452 (1969) (Douglas, J., concurring).

Mr. Justice Holmes, though never formally abandoning the “clear and present danger” test, moved closer to the First Amendment ideal when he said in dissent in *Gitlow v. New York*, 268 U.S. 652, 673 (1925):

“Every idea is an incitement. It offers itself for belief, and, if believed, it is acted on unless some other belief outweighs it or some failure of energy stifles the movement at its birth. The only difference between the expression of an opinion and an incitement in the narrower sense is the speaker’s enthusiasm for the result. Eloquence may set fire to reason. But whatever may be thought of the redundant discourse before us, it had no chance of starting a present conflagration. If, in the long run, the beliefs expressed in proletarian dictatorship are destined to be accepted by the dominant forces of the community, the only meaning of free speech is that they should be given their chance and have their way.”

120. *See* Genesis 4:1–24.

Envy is not one of the motivations recognized by Mill and the act of killing his brother in the presence of an all-powerful God is manifestly against Cain’s own self-interest, yet his desires overcame his enlightened self-interest:

Cain became a farmer and made an offering of his fruit to God. [Abel] became a shepherd and gave the best from his flock of sheep. God smiled upon Abel but not upon Cain. Cain became greatly distressed. God said to Cain, “Why are you sad? You can improve. Now is the time you must choose to act good or bad. Sin lusts after you but you can dominate it. Evil tempts you so that you can learn to master it.”

In time, Cain killed Abel.

Cain and Abel, MY JEWISH LEARNING, <https://www.myjewishlearning.com/article/cain-and-abel-hot-topic/> [<https://perma.cc/ZRG2-STYZ>].

psychological insights if we are to understand our economic actions, including those relating to habits, customs and concerns about social wealth, fairness and justice.”¹²¹

Modern behavior economics is generally attributed to Daniel Kahneman and Amos Tversky, who pioneered the field in the 1970s.¹²² Through their empirical work on portfolio choices, they established that economic assumptions of risk and rationality were largely fallacies. Instead, “Kahneman and Tversky emphasized that choices often depend on the manner in which alternatives are framed.”¹²³ They opened the door to understand how cognitive biases, asymmetric information, and framing choices can manipulate or nudge the seemingly independent decisions made by individuals.¹²⁴

Unfortunately, while behavioral economics can be used to nudge individuals to make better choices, marketers can use these techniques to manipulate individuals to make choices that might be less beneficial to the individual, and unscrupulous actors may seek to manipulate the public for their own gain.

Behavioral economics has been popularized by books such as *Freakonomics* by Steven Levitt & Stephen Dubner,¹²⁵ which provided a comprehensive introduction to the way in which decision making is driven by non-rational biases, assumptions, and cognitive framing strategies. They explained that “[a]n incentive is simply a means of urging people to do more of a good thing and less of a bad thing.”¹²⁶ To this simple explanation of incentives, the book adds an important caveat: “[M]ost incentives don’t come about organically. Someone—an economist or a politician or a parent—has to invent them.”¹²⁷ Three years later, Richard Thaler and Cass Sunstein published *Nudge*, which identifies benevolent behavioral economic incentives to further social good.¹²⁸ Thaler and Sunstein advocated for “libertarian paternalism,” a concept by which individuals are not prescribed by regulations or authoritarian limitations but are nonetheless encouraged to make healthy, socially beneficial

121. GRAHAM MALLARD, BEHAVIOURAL ECONOMICS 16 (2017) (discussing ADAM SMITH, THEORY OF MORAL SENTIMENTS (1759)).

122. Hersh Shefrin & Meir Statman, *The Contributions of Daniel Kahneman and Amos Tversky*, 4 J. BEHAV. FIN. 54 (2003).

123. *Id.* at 55.

124. *See* MALLARD, *supra* note 121, at 75.

125. STEVEN D. LEVITT & STEPHEN J. DUBNER, *FREAKONOMICS: A ROUGE ECONOMIST EXPLORES THE HIDDEN SIDE OF EVERYTHING* (2009).

126. *Id.* at 17.

127. *Id.*

128. RICHARD H. THALER & CASS R. SUNSTEIN, *NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS* (2009).

choices though paternalistic choice architecture that encourages the desired behavioral outcomes.¹²⁹ A nudge, according to Thaler and Sunstein, “is any aspect of the choice architecture that alters people’s behavior in a predictable way without forbidding any options or significantly changing their economic incentives.”¹³⁰

Unfortunately, those who wish to choose to shape public choice in order to exploit members of the public for profit also understand the importance of incentive architecture. Nudges are morally neutral. Those committing fraud often use precisely the same fundamental tools to reinforce cognitive biases and choice architecture to profit off the public to the public’s loss. To capture the range of social harms, researchers have added to the nudge lexicon: “Nudges steer people toward certain options but also allow them to go their own way. ‘Dark nudges’ aim to change consumer behavior against their best interests. ‘Sludge’ uses cognitive biases to make behavior change more difficult.”¹³¹ Dark nudges, they explain, “encourage the consumption of harmful products (for example, by exploiting gamblers’ cognitive biases).”¹³² Dark nudges are then reinforced with “sludge,” to “make behavior change harder.”¹³³

As described below, one type of dark nudge and sludge combination is to promote a medically unproven (or disproven) but easy to follow medical regime. Targets are told to forget expensive medications and instead follow a real doctor’s advice on ‘eating favorite food to find their hidden benefits.’ The doctor’s advice is monetized by selling the information as a combination of books, videos, webinars, and apps. Each is accompanied by false testimonials and multiple false sources that reinforce the message that one can achieve better health without undertaking the difficult lifestyle changes that are actually required to lose weight and stay on prescribed medications.¹³⁴

Psychographic segmentation¹³⁵ is used to profile the target and identify which emotional triggers are most likely to darkly nudge the

129. *Id.* at 5 (“When we use the term libertarian to modify the word paternalism, we simply mean liberty-preserving.”).

130. *Id.* at 6.

131. Mark Pettigrew, Nason Maani, Luisa Pettigrew, Harry Rutter, & May Ci Van Scalkwyk, *Dark Nudges and Sludge in Big Alcohol: Behavioral Economics, Cognitive Biases, and Alcohol Industry Corporate Social Responsibility*, 98 MILBANK Q. 1290, 1290 (2020).

132. *Id.*

133. *Id.*

134. *See, e.g.*, SEEMA YASMIN, VIRAL BS: MEDICAL MYTHS AND WHY WE FALL FOR THEM 9 (2021).

135. *See, e.g.*, *Psychographics: The Key to Motivating Healthcare Consumer Behaviors*, PATIENTBOND, <https://www.patientbond.com/psychographics> [<https://perma.cc/527J-C7RG>] (last visited Nov. 20, 2022). (“Psychographics pertain to people’s attitudes, values, lifestyles and

person towards buying the valueless bad information which has the consequential effect of worsening the individual's actual health and making the person more likely to be in need of more instant health care fixes.¹³⁶ “[D]igital marketing tools . . . include psychographic and neuromarketing tools combined with data and tracking methods (such as emotion-based profiling) to optimise the emotional impact of advertising messages to specific audiences’ psychological needs.”¹³⁷

A study in the field of alcohol consumption (which in excess leads to negative health consequences) highlights the power of dark nudges.

Dark nudges appear to be used in AI communications about “responsible drinking.” The approaches include social norming (telling consumers that “most people” are drinking) and priming drinkers by offering verbal and pictorial cues to drink, while simultaneously appearing to warn about alcohol harms. Sludge, such as the use of particular fonts, colors, and design layouts, appears to use cognitive biases to make health-related information about the harms of alcohol difficult to access, and enhances exposure to misinformation. Nudge-type mechanisms also underlie AI mixed messages, in particular alternative causation arguments, which propose nonalcohol causes of alcohol harms.¹³⁸

The lessons of sludge have long been used in Las Vegas and casino design, whereby, an unarticulated, and perhaps unrecognized collaboration, exists between an addictive gambler and the casino design. Casinos utilize physical spaces that limit external intrusion, lighting and sound that drive the gambler's focus into the digital slot machine, and machines designed to emphasize focus and control. Each choice is

personalities and are the key to understanding healthcare consumers’ motivations and communication preferences. Segmenting people by these characteristics allows you to target and deliver communications that resonate more effectively and increase the likelihood of behavior activation.”).

136. See generally *FTC v. Agora Fin., LLC*, 447 F. Supp. 3d 350, 355 (D. Md. 2020).

137. Vian Bakir, *Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica’s Psychographic Profiling and Targeting*, 5 *FRONTIERS COMM’N*, Sept. 3, 2020, at 1, 4.

Alcohol consumption is a particularly suitable area in which to explore harmful use of cognitive biases for two reasons. First, alcohol is a product that disproportionately harms the most vulnerable, and the alcohol industry is financially reliant on harmful use of its products. Second, there is growing evidence that alcohol industry corporate social responsibility organizations act to misrepresent the evidence on alcohol harms. It has recently been shown that such bodies misrepresent the scientific evidence on alcohol harms in pregnancy.

Petticrew et al., *supra* note 131, at 1296–97.

138. Petticrew et al., *supra* note 131, at 1291.

engineered to maintain a gambling zone where the external world drops away and the only thing that matters is the next bet.¹³⁹

A study of the alcohol industry identifies that the organizations responsible for promoting responsible drinking use dark nudges such as color cues, fonts, website designs, selective omission of key health risks, over-emphasis of minor health risks to diminish the threat of the significant risks, positive images that are inconsistent with the informational warnings being given, and many more similar strategies to devalue the information they provide about the actual health risks from alcohol.¹⁴⁰

The use of dark nudges may help ensure that any health information provided by such organizations has little or no effect on consumers' decisions; effective, unbiased provision of health information would pose too much of a risk to the alcohol market. Multiple dark nudges are therefore used: The positioning of information adds friction and reduces information accessibility, while readers are subject to priming and framing in which minor health effects are prioritized and chronic harms are omitted and reframed. Information overload and dilution with irrelevant trivia are also employed. Sludge also plays a role, for example, through requirements to take complicated sets of actions in order to obtain information, and through the use of layouts and fonts rarely optimized for the browser window.¹⁴¹

These strategies are regularly used throughout health and wellness products in addition to being used by those products that are harmful to health benefits. For example, a marketing firm by the name of "Irrational Agency" has published a blog post touting its ability to nudge doctors into prescribing three times the amount of a particular drug than before its campaign.¹⁴² The marketing company conducted physician interviews to determine "barriers and drivers for prescribing" the drug being marketed, as well as "cognitive-behavioral interviews to explore latent barriers" to prescribing the market drug.¹⁴³ The marketing company then tested potential nudges to identify the four strategies most impactful and

139. See NATASHA DOW SCHÜLL, ADDICTION BY DESIGN: MACHINE GAMBLING IN LAS VEGAS 41–48 (2014). See also Natasha Dow Schüll, *Digital Gambling: The Coincidence of Desire and Design*, 597 ANNALS, AAPSS, no. 1, 2005, at 65.

140. Petticrew et al., *supra* note 131, at 1313.

141. *Id.*

142. See Leigh Caldwell, *Pharma Company Uses Nudges to Triple Sales*, GREENBOOK (April 4, 2019), <https://www.greenbook.org/mr/insights-that-work/pharma-company-uses-nudges-to-triple-sales/> [<https://perma.cc/69JV-NTQT>] (written by Co-Founder & Partner / The Irrational Agency).

143. *Id.*

deployed those four changes.¹⁴⁴ “In the first quarter of the new strategy, revenue increased by two hundred percent – a tripling of sales volume. Using nudges revolutionized the product’s success, with no extra spend on advertising or price promotions.”¹⁴⁵

The marketing company, of course, does not address the efficacy of the drug for the patients. Its goal was to increase prescription rates, and it found effective cognitive-behavioral nudges to significantly motivate the prescribing doctors. These techniques have become ubiquitous, and their consequences are largely ignored.

The FTC has started to take steps at least to acknowledge the problem. In September 2022, it released a report entitled “Bringing Dark Patterns to Light,”¹⁴⁶ which captures many of the same sludge techniques to reduce consumer response to adverse information and undermine the messages of warnings or other qualifiers. The FTC also adds such techniques as:

- Misleading Consumers and Disguising Ads.
- Making it difficult to cancel subscriptions or charges.
- Burying key terms and junk fees.
- Tricking consumers into sharing data.¹⁴⁷

The FTC uses the term “dark patterns” to “describe design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm.”¹⁴⁸ The false information promoted through dark patterns is particularly troubling:

Some dark patterns manipulate consumer choice by inducing false beliefs. For example, a company may make an outright false claim or employ design elements that create a misleading impression to spur a consumer into making a purchase they would not otherwise make. Classic examples of these types of deceptive dark patterns include advertisements deceptively formatted to look like independent, editorial content and purportedly neutral comparison-shopping sites that actually rank companies based on compensation. Workshop panelists also discussed countdown timers on offers that are not actually time-limited, claims that an item is almost sold out when there is actually ample

144. *Id.*

145. *Id.*

146. *Bringing Dark Patterns to Light*, FTC BUREAU OF CONSUMER PROT. (Sept. 15, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers> [<https://perma.cc/VSG2-UFDL>].

147. *Id.*

148. *Id.* at 2 (using the term coined by design specialist Harry Brignull).

supply, and false claims that other people are also currently looking at or have recently purchased the same product.¹⁴⁹

As with the techniques identified in the alcohol industry, other dark patterns or sludges include- hiding disclosures or disclaimers, charging for services listed as free, making information difficult to notice by placing it “below the fold” or low down on a website, burying information in plain text amidst bolded type, and a myriad of similar strategies.¹⁵⁰

The FTC has had some limited success for fraudulent collection of fees using these techniques as well as for false advertising, but as noted in the next section, those successes are highly constrained because of the First Amendment protections for speech, even if it includes manipulative dark patterns or sludges intended to interfere with true individual autonomy.

IV. THE FTC’S ROLE IN POLICING UNFAIR AND DECEPTIVE TRADE PRACTICES

Congress, regulators, and courts have known such manipulative behavior affecting the public’s health has been going on for a very long time. One of the earliest laws was the Pure Food and Drug Act of 1906 (“1906 Act”): “An Act for preventing the manufacture, sale, or transportation of adulterated or misbranded or poisonous or deleterious foods, drugs, medicines, and liquors, and for regulating traffic therein, and for other purposes.”¹⁵¹ Congress supplemented this authority by passing the FTC Act in 1914 to protect the public from the broader category of unfair and deceptive trade practices.¹⁵²

Deceptive “practices . . . involv[e] a material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances. An act or practice is “unfair” if it “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”¹⁵³

149. *Id.* at 4 (internal citations omitted).

150. *Id.* at 7.

151. Pure Food and Drug Act, Pub. L. No. 59-384, 34 Stat. 768 (1906) (codified at 21 U.S.C. §§ 1–15 (1934) (repealed 1938)). See Chelsea M. Childs, *Federal Regulation of the “Smart Choices Program”*: *Subjecting Front-of-Package Nutrition Labeling Schemes to Concurrent Regulation by the FDA and the FTC*, 90 B.U. L. REV. 2403, 2406 (2010).

152. 15 U.S.C. § 45 (2022).

153. *A Brief Overview of the Federal Trade Commission’s Investigative, Law Enforcement, and Rulemaking Authority*, FTC, <https://www.ftc.gov/about-ftc/mission/enforcement-authority>

The 1906 Pure Food and Drug Act and general authority of the FTC were updated in 1938 with the Federal Food, Drug, and Cosmetic Act (“FDCA”) in 1938.¹⁵⁴

The Federal Trade Commission is a law enforcement agency charged by Congress with protecting the public against anticompetitive behavior and deceptive and unfair trade practices. . . . The Commission also has the authority under Section 13(b) of the FTC Act to seek a preliminary injunction in federal district court whenever the Commission has reason to believe that a party is violating, or is about to violate, any provision of law enforced by the FTC. . . . Additionally, the Commission has the authority to seek a permanent injunction in federal district court in a “proper case” pursuant to section 13(b) of the FTC Act.¹⁵⁵

The FTC authority under the FDCA provides important safeguards for protecting the marketplace from products that are unsafe for the public.¹⁵⁶ As a criminal statute, the FDCA requires that “object of the violation must be a ‘food,’ ‘drug,’ ‘device,’ or ‘cosmetic.’”¹⁵⁷ The item must be in interstate commerce, and it must meet the test for being “adulterated” or “misbranded.”¹⁵⁸ Apps and similar software intended “for maintaining or encouraging a healthy lifestyle and is unrelated to the diagnosis, cure, mitigation, prevention or treatment of a disease or condition,” are statutorily excluded from the definition of devices subject to the FDCA.¹⁵⁹ Given this definition, the FDCA provides little assistance to manage the disinformation and data misuse issues.

In addition, the authority over drugs and medical devices does not extend to off-label use of approved drugs, the practice of medicine, or the

[<https://perma.cc/E67T-PXG2>] (quoting 15 U.S.C. § 45(n) (unfair); FTC Policy Statement on Deception, in *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984) (summarizing deceptive)).

154. 21 U.S.C. § 301 (2006). *See also* U.S. v. *Dotterweich*, 320 U.S. 277, 280 (1943) (“The Food and Drugs Act of 1906 was an exertion by Congress of its power to keep impure and adulterated food and drugs out of the channels of commerce. By the Act of 1938, Congress extended the range of its control over illicit and noxious articles and stiffened the penalties for disobedience.”).

155. Markus Meier, Bradley Albert & Kara Monahan, *Overview of FTC Actions in Health Care Services and Products*, FTC BUREAU OF COMPETITION, HEALTH CARE DIVISION 1 (June 2019), https://www.ftc.gov/system/files/attachments/competition-policy-guidance/overview_health_care_june_2019.pdf [<https://perma.cc/E4TP-RWZQ>].

156. *See, e.g.*, Anna B. Laakmann, *Customized Medicine and the Limits of Federal Regulatory Power*, 19 VAND. J. ENT. & TECH. L. 285, 286 (2016) (“The FDCA gives the US Food and Drug Administration (FDA) enormous power to determine which products are brought to market and how those products are manufactured, promoted, and distributed to hospitals, physicians, and patients.”).

157. Megan Hanley Baer & Whitney Moore, *Federal Food and Drug Act Violations*, 40 AM. CRIM. L. REV. 613, 614–15 (2003); 21 U.S.C. § 331(a) (2022).

158. 21 U.S.C. § 331(a) (2022).

159. 21 U.S.C. § 321(h); 21 U.S.C. § 360j(o)(1)(B).

advice provided by medical practitioners.¹⁶⁰ Congress intended to leave the practice of medicine to state regulators, which further limits the authority of the FTC to stop even intentional disinformation regarding health claims.

Although the FDCA is focused on a different set of health protections, the FTC still has some power to protect the public, particularly with regard to unfair and deceptive trade practices involving the theft of customer data and the lax practices that allow that data to be stolen in those situations not otherwise covered by the OCR.¹⁶¹

“The FTC has used this authority to establish the broadest and most impactful jurisprudence in the area of information privacy, contending in guidance and through enforcement actions that consumers are entitled to ‘fair information practices,’ such as notice, choice, access, accuracy, data minimization, security, and accountability.”¹⁶² The FTC had demonstrated its authority through litigation and administrative actions to establish authority to use the general power of Section 5 to prohibit companies from failing to protect customer data,¹⁶³ as well as from failing to adhere to the company’s own statements regarding the use of customer data.¹⁶⁴ Congress has extended this authority in the context of online

160. See Lars Noah, *Ambivalent Commitments to Federalism in Controlling the Practice of Medicine*, 53 U. KAN. L. REV. 149, 159 (2004) (“The Supreme Court long ago recognized that the police powers of the states justified their regulation of the practice of medicine.”). See also Laakmann, *supra* note 155, at 295; Legal Status of Approved Labeling for Prescription Drugs; Prescribing for Uses Unapproved by the Food and Drug Administration, 37 Fed. Reg. 16,503, 16, 503 (“Once a new drug is in a local pharmacy after interstate shipment, the physician may, as part of the practice of medicine, lawfully prescribe a different dosage for his patient, or may otherwise vary the conditions of use from those approved in the package insert, without informing or obtaining the approval of the Food and Drug Administration.”); 21 U.S.C. § 396 (2012) (“Nothing in this chapter shall be construed to limit or interfere with the authority of a health care practitioner to prescribe or administer any legally marketed device to a patient for any condition or disease within a legitimate health care practitioner-patient relationship.”).

161. See James T. Kitchen, David R. Coogan & Keeton H. Christian, *The Evolution of Legal Risks Pertaining to Patch Management and Vulnerability Management*, 59 DUQ. L. REV. 269, 292 (2021) (“Like the FTC, the HHS OCR has also demonstrated an interest in investigating and bringing enforcement actions for vulnerability management and patch management practices.”).

162. Hillary Brill & Scott Jones, *Little Things and Big Challenges: Information Privacy and the Internet of Things*, 66 AM. U.L. REV. 1183, 1208 (2017).

163. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257 (3d Cir. 2015) (upholding FTC’s authority under Section 5 to bring civil complaint for hotel’s failure to provide any firewalls or other data security measures).

164. See generally FTC, Privacy and Security Enforcement (last visited Nov. 15, 2022), <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement> [<https://perma.cc/YWN7-SR7F>] (listing cases); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600 (2014) (“Today, the FTC is viewed as the de facto federal data protection authority. A data protection authority is common

protection of children’s privacy,¹⁶⁵ as well as in the field of financial privacy.¹⁶⁶ Congress has not directly addressed the FTC’s authority over privacy and cybersecurity outside of these specific fields, but recently, it has proposed legislation to affirm and expand such authority.¹⁶⁷ Perhaps because of the nature of the FTC’s congressional authority¹⁶⁸ and the rather limited Magnuson-Moss rulemaking authority under Section 5,¹⁶⁹ the FTC guides more than it legislates.¹⁷⁰ The FTC has begun to explore more aggressive rulemaking, but its past three decades have been defined by substantial informal guidance to shape industry practices that, along with its limited enforcement actions, may help steer the more conscientious enterprises. These efforts, however, have done little to stop the intentional disinformation, hucksterism, and willfully lax practices of the market.

Recently, the FTC has targeted health care app privacy failures. In February 2023, the FTC filed a complaint against GoodRx for violating

in the privacy law of most other countries, which designate a particular agency to have the power to enforce privacy laws.”).

165. 15 U.S.C. §§ 6501–6506 (2022); 16 Fed. Reg. 312 (Children’s Online Privacy Protection Act).

166. 15 U.S.C. §§ 6801 (2022); 65 Fed. Reg. 33677 (Privacy of Consumer Financial Information).

167. *See, e.g.*, The American Data Privacy and Protection Act (ADPPA), H.R. 8152, 117th Cong. (2022) (on July 20, 2022, the House Energy and Commerce Committee voted 53-2 to advance the legislation to the floor).

168. *See* 15 U.S.C. § 57a (2022); Magnuson-Moss Warranty — Federal Trade Commission Improvement Act, Pub. L. No. 93-637, 88 Stat. 2183 (1975) (codified as amended in scattered sections of 15 U.S.C.); Dan Bosch, *Primer: The FTC and Magnuson-Moss Rulemaking*, INSIGHT (Sept. 21, 2022).

Congress gave the FTC authority to issue regulations that could apply industry-wide with the Magnuson-Moss Warranty – Federal Trade Commission Improvement Act of 1975 In recognizing the broad authority it granted the FTC, the Magnuson-Moss Act imposed some additional rulemaking steps on the agency beyond those typical of the common informal rulemaking described in the Administrative Procedure Act (APA). . . . In 1980, Congress enacted . . . additional steps for the agency to follow to prevent the issuing of excessive rules by making the process more exacting on the FTC, thus disincentivizing (or perhaps appropriately incentivizing) broad rulemakings in favor more targeted enforcement of specific abuses.

See also Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-252, 94 Stat. 374 (1980) (adding obligation to complete an advance notice of rulemaking with submission of such proposal to House and Senate committees as an additional rulemaking step along with other new procedural requirements).

169. *See* Rohit Chopra & Lina M. Khan, *The Case for “Unfair Methods of Competition” Rulemaking*, 87 U. CHI. L. REV. 357, 369 (2020) (“[A] common misconception is that this authority is extremely limited because FTC rulemaking is subject to the extensive hurdles posed by the Magnuson-Moss Warranty-Federal Trade Commission Improvements Act.”).

170. *Id.* at 370 (arguing that the FTC does have authority under the Administrative Practice Act to conduct rulemaking involving “unfair methods of competition”).

its published terms of service and providing Facebook with its customers' personal information.¹⁷¹ The complaint alleges that GoodRx "promised its users that it would . . . never share personal health information with advertisers or other third parties."¹⁷² Instead, "GoodRx repeatedly violated these promises, however, by sharing sensitive user information with third-party advertising companies and platforms ("Advertising Platforms") like Facebook, Google, and Criteo, and other third parties like Branch and Twilio."¹⁷³ Within three weeks of filing the complaint, the FTC settled with GoodRx. "The stipulated order entered by the Court on Feb. 17 requires GoodRx to pay a civil penalty of \$1.5 million and to take corrective action to prevent future unauthorized disclosure of users' sensitive health information and to ensure compliance with the FTC Act and rules."¹⁷⁴ While this is a significant victory for the FTC, the action against GoodRx comes from the company's failure to adhere to its own privacy policies and does not address the accuracy of its content.

The reason the FTC emphasizes deceptive practices such as violations of a company's own privacy policy is because the FTC has much less over unfair practices than deceptive practices. In 1994, amendments to the FTC Act prohibited the FTC from declaring "unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."¹⁷⁵

In sum, while the FTC has done a great deal to set the tone for appropriate regulation, it is severely limited in its authority. The statutes that empower the FTC to regulate food and drugs do not extend to apps and publications. The rulemaking is highly constrained. And there is a philosophical need to restrain regulation to reflect the right of an individual to make even poor health decisions. As such, the FTC is not presently in a position to achieve any significant impact on the disinformation in the health care sector.

171. Complaint at 2–4, *United States v. GoodRx Holdings, Inc.*, No. 23-cv-460 (N.D. Cal. Feb. 1, 2023).

172. *Id.* at 2.

173. *Id.*

174. Press Release, Dept. of Justice, Digital Healthcare Platform Ordered to Pay Civil Penalties and Take Corrective Action for Unauthorized Disclosure of Personal Health Information (Feb. 22, 2023), <https://www.justice.gov/opa/pr/digital-healthcare-platform-ordered-pay-civil-penalties-and-take-corrective-action> [<https://perma.cc/DJY8-ZRBZ>].

175. 15 U.S.C. § 45(n) (2022).

The FTC has recently won victories against POM Wonderful, LLC for making false and deceptive health claims regarding its pomegranate-based juice and other products.¹⁷⁶ The D.C. Circuit explained that “[t]he FTC Act proscribes—and the First Amendment does not protect—deceptive and misleading advertisements. Here, we see no basis for setting aside the Commission’s conclusion that many of POM’s ads made misleading or false claims about POM products.”¹⁷⁷

The court explained the nature of the structure of the inquiry that must occur for the FTC to establish its claims that the defendant is violating Section 5 as a three-step inquiry. The FTC considers “(i) what claims are conveyed in the ad, (ii) whether those claims are false, misleading, or unsubstantiated, and (iii) whether the claims are material to prospective consumers.”¹⁷⁸

In identifying the claims made by an ad, the Commission distinguishes between “efficacy claims” and “establishment claims.” An efficacy claim suggests that a product successfully performs the advertised function or yields the advertised benefit, but includes no suggestion of scientific proof of the product’s effectiveness. An establishment claim, by contrast, suggests that a product’s effectiveness or superiority has been scientifically established.

The distinction between efficacy claims and establishment claims gains salience at the second step of the Commission’s inquiry, which calls for determining whether the advertiser’s claim is false, misleading, or unsubstantiated. If an ad conveys an efficacy claim, the advertiser must possess a “reasonable basis” for the claim. The FTC examines that question under the so-called “*Pfizer* factors,”¹⁷⁹ including “the type of product,” “the type of claim,” “the benefit of a truthful claim,” “the ease of developing substantiation for the claim,” “the consequences of a false claim,” and “the amount of substantiation experts in the field would consider reasonable.”¹⁸⁰

For establishment claims, by contrast, the Commission generally does not apply the *Pfizer* factors. Rather, the amount of substantiation needed

176. *POM Wonderful, LLC v. FTC*, 777 F.3d 478, 483–84 (D.C. Cir. 2015) (“[F]rom 2003 to 2010, POM touted medical studies ostensibly showing that daily consumption of its products could treat, prevent, or reduce the risk of various ailments, including heart disease, prostate cancer, and erectile dysfunction. Many of those ads mischaracterized the scientific evidence concerning the health benefits. . . .”).

177. *Id.* at 484.

178. *Id.* at 490 (citing *Kraft, Inc. v. FTC*, 970 F.2d 311, 314 (7th Cir. 1992)).

179. See *Pfizer Inc.*, 81 F.T.C. 23, 62 (1972).

180. *POM Wonderful*, 777 F.3d at 490–91 (quoting Daniel Chapter One, No. 9329, 2009 WL 5160000, at *25 (U.S. Fed. Trade Comm’n Dec. 24, 2009) (other citations omitted)).

for an establishment claim depends on whether the claim is “specific” or “non-specific.” If an establishment claim “states a specific type of substantiation,” the “advertiser must possess the specific substantiation claimed.”¹⁸¹ If an ad instead conveys a non-specific establishment claim—e.g., an ad stating that a product’s efficacy is “medically proven” or making use of “visual aids” that “clearly suggest that the claim is based upon a foundation of scientific evidence”—the advertiser “must possess evidence sufficient to satisfy the relevant scientific community of the claim’s truth.”¹⁸²

The Commission therefore “determines what evidence would in fact establish such a claim in the relevant scientific community” and “then compares the advertisers’ substantiation evidence to that required by the scientific community.”¹⁸³ Even if the Commission concludes at the first step that an advertiser conveyed efficacy or establishment claims and determines at the second step that the claims qualify as false, misleading, or unsubstantiated, it can issue a finding of liability only “if the omitted information would be a material factor in the consumer’s decision to purchase the product.”¹⁸⁴

Applying this three-part test, the D.C. Circuit Court found that POM Wonderful’s use of ads to tout medical benefits of the product to cure heart disease, prostate cancer, or erectile dysfunction, were never supported by the scientific studies that were funded by the company. To the contrary, all preliminary studies of benefit were not substantiated in broader trials, so the ads simply ignored those broader studies.¹⁸⁵

According to that ad, POMx is “backed by \$34 million in medical research at the world’s leading universities” revealing “promising results for erectile, prostate and cardiovascular health.” *Id.* The ad goes on to discuss three specific studies: Dr. Padma–Nathan’s erectile dysfunction study, Dr. Pantuck’s PSA doubling time study, and Dr. Ornish’s blood flow study. Of the first, the ad says that, “[i]n a preliminary study on erectile function, men who consumed POM Juice reported a 50% greater likelihood of improved erections as compared to placebo.”¹⁸⁶

181. *Id.* at 491 (quoting *Removatron Int’l Corp.*, 884 F.2d 1489, 1492 n.3 (1st Cir. 1989)).

182. *Id.* (quoting *Bristol–Myers Co.*, 102 F.T.C. 21, 321 (1983), *aff’d*, 738 F.2d 554 (2d Cir. 1984)).

183. *Id.* (quoting *Removatron*, 884 F.2d at 1498).

184. *Id.* (quoting *Am. Home Prods. Corp.*, 98 F.T.C. 136, 368 (1981), *enforced as modified*, 695 F.2d 681 (3d Cir. 1982)).

185. *See id.* at 490–92.

186. *Id.* at 492.

Later studies, however, did not substantiate these preliminary findings. At the FTC administrative hearing, “the Commission found that ‘experts in the relevant fields’ would require one or more ‘properly randomized and controlled human clinical trials’—‘RCTs’—in order to ‘establish a causal relationship between a food and the treatment, prevention, or reduction of risk’ of heart disease, prostate cancer, or erectile dysfunction.”¹⁸⁷ The substantiation of these claims requires at least these levels of evidence to support the requirements.¹⁸⁸ As a result, despite the numerous objections preferred by POM Wonderful, the court found that the substantiation of the claims was substantially lacking, and that these unsubstantiated claims were material to the consumers subject to injunctive relief by the court.

The court then applied the Central Hudson test for intermediate scrutiny of commercial speech.¹⁸⁹ The court further noted that “[m]isleading advertising may be prohibited entirely.”¹⁹⁰ The court still treated the misleading and substantiated claims to the protection of Central Hudson. The court addressed the need for the FTC’s remedial injunction to serve the substantial interest of the government in accurate health information.

Next, the court required that the FTC’s remedial injunction provide an appropriate fit between the speech to be restricted and the government’s interest. As the court noted, “*Central Hudson* requires that a challenged restriction ‘directly advance[] the governmental interest’ and that it ‘is not more extensive than is necessary to serve that interest.’”¹⁹¹ The court was in agreement with the FTC that the RCTs were

187. *Id.* at 493–94.

188. Randomized and controlled human clinical trials are the heart of the competent and scientifically reliable evidence required by the FTC. *See, e.g.*, *FTC v. Agora Fin., LLC*, 447 F. Supp. 3d 350, 360 (D. Md. 2020) (advertisement for wellness guide). In *Agora*, the FTC listed additional examples: *FTC v. Alcoholism Cure Corp.*, No. 3:10-cv-266-J-34JBT, 2011 WL 13137951 (M.D. Fl. Sept. 16, 2011) (selling participation in an ongoing, monthly alcoholism cure program and representing that the program “cures alcoholism for most alcoholics who sign up for the program” and “cures alcoholism while allowing alcoholics to drink socially”); *FTC v. Nat’l Urological Grp., Inc.*, 645 F. Supp. 2d 1167, 1177 (N.D. Ga. 2008) (selling weight loss and/or erectile performance dietary supplements); *FTC v. NPB Advertising, Inc.*, 218 F. Supp. 3d 1352, 1359 (M.D. Fl. 2016) (selling green coffee extract as a dietary weight-loss supplement); *FTC v. Roca Labs, Inc.*, 345 F. Supp.3d 1375, 1381, 1387–89 (M.D. Fl. 2018) (selling various weight loss products, including “formula” and “anti-cravings”); *FTC v. Direct Marketing Concepts, Inc.*, 569 F. Supp. 2d 285, 303–04 (D. Mass. 2008) (selling herbal dietary supplements).

189. *POM Wonderful*, 777 F.3d at 499 (quoting *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n*, 447 U.S. 557, 566 (1980) (“For commercial speech to come within [the First Amendment], it at least must concern lawful activity and not be misleading.”)).

190. *Id.* (quoting *In re R.M. J.*, 455 U.S. 191, 203 (1982)).

191. *Id.* at 501 (quoting *Cent. Hudson*, 447 U.S. at 566).

appropriate to meet the fit or tailoring requirement of *Central Hudson*. At the same time, however, where the FTC had sought to impose a minimum of two controlled studies on future claims, the court rejected this prescriptive limitation on the defendant. The court noted that certain well-designed trials can be conclusive in a single, large, and well-designed study such that the imposition of two such studies was an unnecessary burden on speech. As a result, despite the victory by the FTC, its authority to reign in blatantly false information was still circumscribed by the court.

The FTC was similarly limited in its successful prosecution of another Section 5 violation. This case involved Agora Financial, LLC (“Agora”) and NewMarket Health, LLC (“NewMarket”), their principals, and more than eighty additional entities used to promote the unfair and deceptive marketing strategies adopted by the criminal enterprise.¹⁹² The fraud committed followed the same model, once involving health related claims and another instance involving financial get-rich-quick schemes.¹⁹³

In August 2018, NewMarket began to promote “The Doctor’s Secret to REVERSING Diabetes in 28 Days” (“The Doctor’s Guide”), a newsletter written by Dr. Richard Gerhauser, MD to promote his “eleven-module protocol for treatment of Type 2 Diabetes without pharmaceuticals.”¹⁹⁴ Through emails, internet banner advertisements, and the defendants’ other publications, the defendants promoted The Doctor’s Guide.¹⁹⁵ The Doctor’s Guide promised revolutionary breakthroughs in curing Type 2 Diabetes:

- “Because after 37 years in practice, I recently discovered a simple, at-home treatment for Type 2 diabetes. And no, it has nothing to do with diet or exercise. It doesn’t involve a single drug either. Yet this new treatment is scientifically proven to reverse every symptom of your diabetes in 28 days.”
- “World famous doctor and diabetes expert, Dr. Richard Gerhauser, just made a shocking announcement. He said ‘Type II Diabetes is not caused by what you eat.’”
- “Shocking study shows 100% cure rate.”
- “It has nothing to do with changing your diet or exercising more.”

192. See *FTC v. Agora Fin., LLC*, 447 F. Supp. 3d 350, 355 (D. Md. 2020).

193. This article will focus on the health charges.

194. *Agora Fin.*, 447 F. Supp. 3d at 355–56.

195. *Id.*

- “Can this new treatment really reverse Type II Diabetes in 28 days? Without diet, exercise, or a single drug? Sure, it sounds impossible . . . But according to a new study from the University of Kansas, it’s true . . .”
- “How to Reverse Diabetes Without Dieting.”¹⁹⁶

Unsurprisingly, these statements were not subject to substantiation. The ads led not only to the sales of *The Doctor’s Guide*, but also to auto-renewing subscriptions to newsletters, to having contact information sold to other confidence solicitors, and a similar cycle of predation.

In the court proceedings, the FTC attempted to follow the procedures identified in *POM Wonderful*, specifically requiring that advertisers “establish that health-related assertions are not misleading, advertisers must have ‘competent and reliable scientific evidence,’ or ‘CRSE,’ to support their claims.”¹⁹⁷

The district court disagreed.

In this case, Defendants have not attempted to sell a product that they claim will yield particular benefits. Rather, Defendants advertised a book that provides, in their view, recommendations on how individuals might reduce the risks and symptoms associated with Type 2 diabetes. In the cases cited by the FTC, the respective defendants marketed products that would be sold for the buyer to consume, and purportedly reap the alleged benefits. The FTC has not identified any case in which a court has applied the health-related efficacy standard in the circumstances presented here.

The dearth of case law in a factually analogous circumstance is likely attributable to First Amendment considerations, which Defendants properly invoke.¹⁹⁸

Moreover, even the FTC elected not to regulate *The Doctor’s Guide*.¹⁹⁹

Regarding the advertisements that led consumers to buy the book and to become part of the market scheme by the eighty companies used to promote these schemes, the court took a very narrow view of the FTC’s scope. “[I]n determining whether Defendants have made any false, fraudulent, or misleading commercial claims here, this Court is not persuaded that its inquiry must include whether the medical claims within *The Doctors’ Guide* are supported by CRSE.”²⁰⁰ The book, is all but

196. *Id.*

197. *Id.* at 360.

198. *Id.* at 361.

199. *Id.* (“The FTC expressly concedes in this case that it seeks only to regulate Defendants’ advertising of *The Doctor’s Guide*, not the content of the publication itself.”).

200. *Id.* at 364.

immune from regulation under the First Amendment, according to the court.

The court does acknowledge that it is subject to “the highest level of protection,” but does not apply the actual malice test, which, in other contexts, allows for tort liability to attach to publications if those publications are made with “knowledge that [the publication] was false or with reckless disregard of whether it was false or not.”²⁰¹ Had this been the standard for *The Doctor’s Guide*, it would have led to an analysis of whether CRSE and CRT is essential to establish reckless disregard of falsity in the publication and remained consistent with decades of First Amendment jurisprudence regarding the regulation of false publications.²⁰²

Earlier cases had little success using Uniform Commercial Code Article 2 warranties to assert publisher liability.²⁰³ Courts have also refused publisher liability for potential negligence in the information published by newspaper columnists.²⁰⁴ At the same time, however, few cases have involved questions about knowing falsehoods in the published materials.

In *Cardozo v. True*, which involved a reader becoming ill after following a recipe to prepare what turned out to be poisonous mushrooms, the court refused to find liability under a theory of merchantability for goods but demurred on the question about publishing knowingly false information.

We make no statements concerning the liability of an author or publisher under the facts as certified to us. Nor do we pass upon the question of whether *Ellie’s* could be held liable if it actually knew the book it sold contained recipes with poisonous ingredients. Rather, we hold that absent allegations that a book seller knew that there was reason to warn the public as to contents of a book, the implied warranty in respect to sale of books by a merchant who regularly sells them is limited to a

201. *Bose Corp. v. Consumers Union of U.S., Inc.*, 466 U.S. 485, 492 (1984); *New York Times Co. v. Sullivan*, 376 U.S. 254, 279–80 (1964).

202. *See Alm v. Van Nostrand Reinhold Co., Inc.*, 480 N.E.2d 1263, 1266 (Ill. App. Ct. 1985) (“Plaintiffs concede that they have discovered no case in any jurisdiction which has imposed liability on a publisher for negligent misrepresentation merely because of the publication of material written by a third party.”).

203. *See Cardozo v. True*, 342 So. 2d 1053, 1056 (Fla. Dist. App. 1977) (denying liability under § 2-316 (Section 672.314, Florida Statutes) for merchantable goods). *See also Yuhas v. Mudge*, 322 A.2d 824 (N.J. 1974) (Popular Mechanics Corp. could not be held liable for an advertisement in the magazine for fireworks that were later found to be defective.).

204. *See, e.g., Mac Kown v. Ill. Publ’g & Printing Co.*, 6 N.E.2d 526 (Ill. App. Ct. 1937) (physician’s dandruff remedy allegedly injured a reader, but the newspaper was not responsible for the injury).

warranty of the physical properties of such books and does not extend to the material communicated by the book's author or publisher.²⁰⁵

Courts have been willing to entertain liability when a publisher provides a seal of endorsement, such as the Good Housekeeping Magazine's Good Housekeeping Seal.²⁰⁶ More generally, websites and radio shows have been found to be liable for defamatory statements which use the same actual malice standard for public figures and negligence standard for private figures.²⁰⁷

The standard for publishers is a high one, and if the publisher is unrelated to the speaker, it may be difficult to meet the clear and convincing evidence standard that a publisher is liable for the publications of its author. "The law is clear . . . that a book publisher has no independent duty to investigate an author's story unless the publisher has actual, subjective doubts as to the accuracy of the story."²⁰⁸

Nonetheless, as illustrated in the cases finding reckless falsity against Alex Jones, InfoWars.com, and Jones's syndicated radio show, multiple juries have been able to find liability under the *New York Times* actual malice standard.²⁰⁹ Nothing suggests that a book publisher or app publisher should be held to yet a higher standard.

The facts in the published opinion do not make clear whether the FTC elected not to proceed against The Doctor's Guide because it was written without the outrageous claims of the advertisements, the inclusion of reasonable advice made it ambiguous as to the level of falsity, or

205. *Cardozo*, 342 So. 2d at 1057.

206. *Hanberry v. Hearst Corp.*, 81 Cal. Rptr. 519, 522 (Cal. Ct. App. 1969) ("Hearst has placed itself in the position where public policy imposes upon it the duty to use ordinary care in the issuance of its seal and certification of quality so that members of the consuming public who rely on its endorsement are not unreasonably exposed to the risk of harm."). *But see Dekens v. Underwriters Laboratories Inc.*, 132 Cal. Rptr. 2d 699, 707 (Cal. Ct. App. 2003) (distinguishing *Hanberry* in an action against Underwriters Laboratory because U.L. could not be responsible to failing to test devices that used asbestos for their medical safety or certify they would not cause cancer when no such affirmative statement was made).

207. *See, e.g., Jones v. Pozner*, No. 03-18-00603-CV, 2020 WL 1809855, at *6 (Tex.) ("Statements by Alex Jones and InfoWars in the 'Sandy Hook Vampires Exposed' video were recklessly false."); *Zedan v. Bailey*, 522 F. Supp. 3d 1363, 1373 (M.D. Ga. 2021); *Atlanta Journal-Constitution v. Jewell*, 555 S.E.2d 175, 183 (2001); *Stern v. Cosby*, 645 F. Supp. 2d 258 (S.D.N.Y. 2009). *See generally Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974) (applying negligence action for a case involving a non-public figure); *Rosenbloom v. Metromedia, Inc.*, 403 U.S. 29 (1971).

208. *Stern*, 645 F. Supp. 2d at 284. *See Lohrenz v. Donnelly*, 350 F.3d 1272, 1284 (D.C. Cir. 2003); *Geiger v. Dell Pub. Co.*, 719 F.2d 515, 518 (1st Cir. 1983); *Hotchner v. Castillo-Puche*, 551 F.2d 910, 914 (2d Cir. 1977).

209. *See Alex Jones, Infowars, and the Sandy Hook Defamation Suits*, FIRST AMEND. WATCH N.Y. UNIV., <https://firstamendmentwatch.org/deep-dive/alex-jones-infowars-and-the-sandy-hook-defamation-suits/> [<https://perma.cc/QN58-X8CU>].

because the Doctor's Guide was actually appropriate health advice marketed in an outrageous and fraudulent manner. Certainly, the court identified statements that contradicted some of the falsehoods of the advertising, which suggests that the book might have been far less inaccurate than the ads. But the opinion does not absolve the book because the book was written with care. The opinion absolves the book because it is a book. In doing so, it suggests that the FTC can only address false advertising, which is a small segment of the unfair and deceptive practices.

The values of the First Amendment for the dissemination of knowledge are axiomatic, and the jurisprudence of the First Amendment makes clear that while falsity is not valuable speech, the law will afford great leniency on potentially inaccurate speech to promote the marketplace of ideas. This important point reemphasizes the right of the individual to access information and make independent decisions regarding the truth or falsity of that which is provided.

V. LIMITS ON HEALTH CARE INFORMATION REFORM: COMMERCIAL FREE SPEECH JURISPRUDENCE

At present, both legislation from Congress and FTC rulemaking steps suggest that new regulations may be in the offing to help empower the FTC to do more about the dark patterns, use of sludge practices, and misuse of health data to improve the regulation of health information. However, even assuming those legislative and regulatory efforts are successful, there remains a significant barrier to enforcement, which is the present jurisprudence which regulates commercial speech.

In recent years, the Supreme Court has moved beyond the balancing approach of *Central Hudson*²¹⁰ towards a heightened standard of First Amendment scrutiny²¹¹ and to a model for strict scrutiny.²¹² However, this standard is not yet clear or applied in a consistent manner by the Supreme Court.²¹³

At the outset, the Supreme Court for decades has found that some commercial speech is protected by the First Amendment, and the question is to what degree that status has changed with the Neo-Lochner Court of the twenty-first century. "The First Amendment, as applied to

210. *Cent. Hudson Gas & Elec. Corp. v. Public Serv. Comm'n*, 447 U.S. 557 (1980).

211. *Sorrell v. IMS Health*, 564 U.S. 552 (2011).

212. *Reed v. Gilbert*, 576 U.S. 155 (2015).

213. *See, e.g., Barr v. Am. Ass'n Pol. Consultants*, 140 S. Ct. 2335 (2020) (plurality); *Iancu v. Brunetti*, 139 S. Ct. 2294 (2019); *Matal v. Tam*, 137 S. Ct. 2012 (2017).

the States through the Fourteenth Amendment, protects commercial speech from unwarranted governmental regulation.”²¹⁴

Beginning with *Sorrell* and expanding with *Reed v. Town of Gilbert*, there has been a focus on the neutrality of the government with regard to the speech it regulates.²¹⁵ In both of these cases, the Supreme Court found that the regulation was content-based rather than content neutral. In *Sorrell*, in particular, the focus for the “heightened scrutiny” was the differentiation based on the speaker. At least potentially, if the law had focused on the harms to which misuse of the health care data had been put, heightened scrutiny would have not been necessary. Harms, unlike speakers, are not subject to strict scrutiny and the Court continues to allow differential harms to be addressed.²¹⁶

Before addressing whether recent case law has amended the test in *Central Hudson*, it is important to first apply that test. At issue in the case was a law that regulated certain content being distributed commercially from the licensed utility. “In December 1973, the [Public Utilities] Commission, appellee here, ordered electric utilities in New York State to cease all advertising that promot[es] the use of electricity.”²¹⁷ Three years later, after the energy crisis of the era had passed, the Commission continued the ban of “all promotional advertising contrary to the national policy of conserving energy.”²¹⁸ In the Court’s opinion, it nowhere distinguishes between content-based and content-neutral regulation of commercial speech. Instead, the Court implicitly assumes that to distinguish between commercial and noncommercial speech, the legislation or ordinance in question is necessarily creating a content-based distinction.

214. *Cent. Hudson*, 447 U.S. at 561 (citing *Va. Pharmacy Bd. v. Va. Citizens Consumer Council*, 425 U.S. 748, 761–62 (1976)).

215. *Sorrell*, 564 U.S. at 565 ([T]he regulation “is designed to impose a specific, content-based burden on protected expression. It follows that heightened judicial scrutiny is warranted.”); *Reed*, 576 U.S. at 171 (“Because the Town’s Sign Code imposes content-based restrictions on speech, those provisions can stand only if they survive strict scrutiny, “which requires the Government to prove that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest.”” (citations omitted)).

216. *Compare* *U.S. v. Alvarez*, 567 U.S. 709 (2012) (The Stolen Valor Act made it a crime to falsely claim receipt of military decorations or medals and provides an enhanced penalty if the Congressional Medal of Honor is involved. Unconstitutional content-based restriction on pure speech), *with* *Giboney v. Empire Storage & Ice Co.*, 336 U.S. 490 (1949) (speech integral to criminal conduct outside First Amendment protection).

217. *Cent. Hudson*, 447 U.S. at 558 (internal quotations omitted).

218. *Id.* at 559.

Instead of focusing on content-based distinctions, the *Central Hudson* Court provided a four-part framework for assessing restrictions on commercial speech:

At the outset, we must determine whether the expression is protected by the First Amendment. For commercial speech to come within that provision, it at least must concern lawful activity and not be misleading. Next, we ask whether the asserted governmental interest is substantial. If both inquiries yield positive answers, we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest.²¹⁹

The balancing test comes into play if, but only if, truthful commercial speech is subject to regulation. If the speech is noncommercial, then strict scrutiny would apply, but under *Central Hudson* if the speech were non-truthful, then there is no constitutional need to restrict the police power of the state to regulate the false information.

More recent cases, such as *Alvarez*, continue to recognize that false speech used to commit crimes remain outside of First Amendment protection.²²⁰ Even though a plurality Court in *Alvarez* applied strict scrutiny to strike down a law barring patently false speech, the Court still distinguished false political speech from speech used to conduct criminal activity. As the Court notes, “the statute seeks to control and suppress all false statements on this one subject in almost limitless times and settings. And it does so entirely without regard to whether the lie was made for the purpose of material gain.”²²¹

The Court is certainly correct that the government cannot merely declare the subject matter of speech criminal and then use that criminality to bar the speech in question. To do so would vitiate the protections of the First Amendment. But even the most expansive protection of free speech by the Court in *Alvarez* does not eliminate the category of unprotected speech that is used to commit fraud, theft, or perjury.²²²

Central Hudson requires that if the speech is deemed truthful commercial speech, then the remaining questions are presented as part of

219. *Id.* at 566. See *Retail Digit. Network, L.L.C. v. Prieto*, 861 F.3d 839, 844 (9th Cir. 2017).

220. *Alvarez*, 567 U.S. at 717 (citing *Giboney*, 336 U.S. at 490).

221. *Id.* at 723 (citing *S.F. Arts & Athletics, Inc. v. United States Olympic Comm.*, 483 U.S. 522, 539–40, (1987) (prohibiting a nonprofit corporation from exploiting the “commercial magnetism” of the word “Olympic” when organizing an athletic competition (internal quotation marks omitted))).

222. *Id.*

the intermediate scrutiny analysis.²²³ The second *Central Hudson* question is the extent to which the regulation advances a substantial government interest.²²⁴ The third question asks whether the regulation actually and directly achieves the goal of the government. Finally, the fourth question asks whether the regulatory solution provides “a fit between the legislature’s ends and the means chosen to accomplish those ends, a fit that is not necessarily perfect, but reasonable, a means narrowly tailored to achieve the desired objective.”²²⁵

The Ninth Circuit has attempted to reconcile the heightened scrutiny of *Sorrell* by placing the increased scrutiny into the meaning of the “fit” test of the third and fourth prongs of *Central Hudson*. It suggests that the differentiation among advertisers and researchers in the Vermont health privacy data regulations suggests that the law was not directly advancing the government’s interest in limiting access to health information, nor was it a good fit to the stated goals of the law.²²⁶

Reed v. Town of Gilbert goes further than *Sorrell* to suggest a new strict scrutiny standard, but this standard may be misplaced.²²⁷ The petitioner in this case was not seeking to promulgate commercial speech at all. As the Court explained, “Petitioners Good News Community Church (Church) and its pastor, Clyde Reed, wish to advertise the time and location of their Sunday church services.”²²⁸ Although the concurrence raises questions as to whether the case should properly have been decided under *Central Hudson*, the content in question has nothing to do with a commercial transaction and the speaker alleging disparate treatment is entitled to more than mere neutrality under the First Amendment, but also to an accommodation to ensure its Free Exercise of Religion is not restricted.²²⁹ Read in this light, the case stands for only the self-evident rule that content based restrictions are generally subject to strict scrutiny.

223. See *Fla. Bar v. Went For It, Inc.*, 515 U.S. 618, 623 (1995) (“Mindful of these concerns, we engage in ‘intermediate’ scrutiny of restrictions on commercial speech, analyzing them under the framework set forth in *Central Hudson*”)

224. *Cent. Hudson Gas & Elec. Corp. v. Public Serv. Comm’n*, 447 U.S. 557, 566 (1980).

225. *Bd. of Trs. of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 477 (1989) (citations and internal quotation marks omitted).

226. *Retail Digit. Network, L.L.C. v. Prieto*, 861 F.3d 839, 849 (9th Cir. 2017) (quoting *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 482 n.2 (1995) (“[B]ecause *Sorrell* applied *Central Hudson*, there is no need for us to ‘craft an exception to the *Central Hudson* standard.’”)).

227. *Reed v. Gilbert*, 576 U.S. 155 (2015).

228. *Id.* at 161.

229. See *Tandon v. Newsom*, 141 S. Ct. 1294 (2021) (requiring accommodation under Free Exercise clause if any other accommodations are provided for any other reasons); *Fulton v. Philadelphia*, 141 S. Ct. 1868 (2021).

To the extent that the heightened protection afforded by the First Amendment requires more exacting scrutiny than that provided by *Central Hudson*, the Court has provided its own answer. In *New York Times v. Sullivan*, the Court distinguished between false speech and false speech that was made with an “actual malice” or “scienter” standard.²³⁰

Even in the publishing context, “[w]hen a distributor acts with the requisite scienter in distributing materials defaming or invading the privacy of a private figure it must be subject to liability. But, a public figure plaintiff may only recover compensatory damages where a distributor acts with ‘actual malice’”²³¹ Actual malice requires the speech was made “with knowledge that it was false or with reckless disregard of whether it was false or not.”²³² Reckless disregard requires substantial culpability. “To have acted with constitutional or actual malice, the defendant must be shown to have had ‘a high degree of awareness of [the statement’s] probable falsity,’ or to have ‘in fact entertained serious doubts as to the truth of his publication.’”²³³

Simply put, whenever a commercial statement is made that is knowingly false or made with a high degree of awareness of the falsity, particularly when the publisher of that statement stands to benefit financially from the disinformation promulgated, then there can be no remaining First Amendment consideration that would stop a regulator from holding the publisher of the disinformation liable. To avoid any chilling of speech, mere misinformation must be tolerated, and good speech should be used to dispel misinformation. But that does not work for disinformation that is intentionally created to exploit the public, when it is embedded using sludge and dark patterns, and when the recipients have been psychographically targeted to maximize the victim’s vulnerability to the false, manipulative information.

Put another way, when misinformation graduates into disinformation because of the intentional or reckless nature of the content producer, then the FTC, states, and law enforcement should be able to enforce the applicable laws without concerns that disinformative content is more heavily regulated than other forms of speech. Laws targeting disinformation should properly be content-based and constitutional for precisely that reason—because they are limited to that speech which is outside the protection of the First Amendment.

230. *New York Times Co. v. Sullivan*, 376 U.S. 254, 280 (1964).

231. *Lerman v. Flynt Distrib. Co., Inc.*, 745 F.2d 123, 139 (2d Cir. 1984).

232. *New York Times*, 376 U.S. at 280.

233. *Lerman*, 745 F.2d at 139 (first quoting *Garrison v. Louisiana*, 379 U.S. 64, 74 (1964), then quoting *St. Amant v. Thompson*, 390 U.S. 727, 731 (1968)).

This standard also has some clear demarcations in practice. The FTC, for example, has clear guidelines regarding the substantiation of advertising claims under Section 5(a) of the FTC Act, which, as noted earlier, prohibits “[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce.”²³⁴ In bringing such claims, the FTC must establish by a preponderance of the evidence that: “(1) there was a representation; (2) the representation was likely to mislead consumers acting reasonably under the circumstances; and (3) the representation was material.”²³⁵ In advertising cases, the question about knowing representations of fact are typically not in dispute. In endorsement and other situations, however, the question of negligent misrepresentations could also become an issue.²³⁶

The standard for determining whether representations of material claims are unfair or deceptive turns on the “reasonable basis” or “substantiation” theory that requires the FTC to show the advertiser “lacked a reasonable basis for making the assertions in its advertisement.”²³⁷ More simply, when an advertiser claims proof of efficacy for its product in an ad, that advertiser must actually have that proof. If the FTC can demonstrate by a preponderance of the evidence that such proof does not exist, then the advertiser has violated Section 5. The advertiser “has the burden of putting forth the substantiation it relied on to support its product claims, but the FTC has the burden of proving that [the advertiser’s] purported substantiation is inadequate.”²³⁸ The FTC has the power to determine what “evidence would in fact establish such a claim in the relevant scientific community.”²³⁹ The FTC “then compares the advertisers’ substantiation evidence to that required by the scientific

234. 15 U.S.C. § 45(a)(1).

235. *FTC v. Innovative Designs, Inc.*, 489 F. Supp. 3d 378, 396–97 (W.D. Pa. 2020) (quoting *FTC v. NHS Svs., Inc.*, 936 F. Supp. 2d 520, 531 (E.D. Pa. 2013)), *aff’d*, 20-3379, 2021 WL 3086188 (3d Cir. July 22, 2021).

236. *See, e.g., The FTC’s Endorsement Guides: Being Up-Front With Consumers*, FTC, <https://www.ftc.gov/news-events/topics/truth-advertising/advertisement-endorsements> [<https://perma.cc/4Y6W-HUKS>].

237. *Innovative Designs*, 489 F. Supp. 3d at 401. *See POM Wonderful, LLC v. FTC*, 777 F.3d 478, 490 (D.C. Cir. 2015).

238. *Innovative Designs*, 489 F. Supp. 3d at 402.

239. *Removatron Intern. Corp. v. FTC*, 884 F.2d 1489, 1498 (1st Cir. 1989).

community.”²⁴⁰ If the FTC can meet this burden, then the advertising violates Section 5,²⁴¹ but, if not, then the advertiser will win the dispute.²⁴²

Most importantly, these standards are not constitutionally limited to advertising. The FTC and other regulators are not prohibited from addressing false factual claims outside the advertising context. This is critically important, since one of the dark patterns common for public manipulation is to create advertorial content that takes on the trappings of editorial content when it has the economic underpinnings of advertising.²⁴³ Even books may be used to further these schemes. A traditionally published book may still be written chock full of unsubstantiated claims that urge readers to buy products or undertake actions that profit the author and harm the reader. The form of the content should not immunize it from prosecution or prohibition.²⁴⁴

Nonetheless, noncommercial speech remains different than commercial speech and efforts to start recharacterizing publications based on their harms would run into the First Amendment concerns which were so problematic in the *Stolen Valor* act.²⁴⁵ Nonetheless, by incorporating the additional protections from *New York Times v. Sullivan* and its line of cases, regulation of the most harmful speech can continue without chilling speech more generally.

This change requires that the regulator meet a clear and convincing standard rather than a preponderance of the evidence standard to find that information was false and created with the requisite actual malice *mens*

240. *POM Wonderful*, 777 F.3d at 490–91 (quoting *Removatron*, 884 F.2d at 1498).

241. *See, e.g., POM Wonderful*, 777 F.3d at 490; *FTC v. Agora Fin., LLC*, 447 F. Supp. 3d 350, 355 (D. Md. 2020).

242. *See, e.g., Innovative Designs*, 489 F. Supp. 3d at 402 (“Because the FTC has not rebutted IDI’s substantiation representations concerning its R-value, it cannot now demonstrate IDI lacked substantiation for its energy saving claims. Thus, the Court finds that the FTC has failed to demonstrate by a preponderance of the evidence that the substantiation IDI had lacked a reasonable basis.”).

243. *Bringing Dark Patterns to Light*, *supra* note 145, at 4 (identifying schemes that falsely claimed editorial content was originating at CNN or Fox). *See also* Susan Gluss, *Duped: Consumers Fooled by Advertorials*, BERKELEY L. (Jan. 14, 2016), <https://www.law.berkeley.edu/article/duped-consumers-fooled-by-advertorials/> [<https://perma.cc/2JTF-AVL9>] (A survey of nearly 600 consumers using an advertorial “embedded in a blog. They found that 27 percent of respondents thought it was written by a reporter or an editor, while another 29 percent weren’t sure. Although the ad was marked “sponsored content,” it failed to raise a red flag.”); Chris Jay Hoofnagle & Eduard Meleshinsky, *Native Advertising and Endorsement: Schema, Source-Based Misleadingness, and Omission of Material Facts*, TECH. SCI. (Dec. 15, 2015), <http://techscience.org/a/2015121503> [<https://perma.cc/PS72-DJYS>].

244. *Schenck v. United States*, 249 U.S. 47, 49–52 (1917) (“The most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic.”), *overruled on other grounds by*, *Brandenburg v. Ohio*, 395 U.S. 444 (1969).

245. *See United States v. Alvarez*, 567 U.S. 709 (2012).

rea.²⁴⁶ The clear and convincing standard requires “evidence indicating that the thing to be proved is highly probable or reasonably certain.”²⁴⁷ If the regulator cannot establish that the assertions of fact were knowingly false, then the regulator might still prevail but only if it can establish that the author or publisher “entertained serious doubts as to the truth” of his statement²⁴⁸ or if the author or publisher possessed a “high degree of awareness of [the publication’s] probable falsity.”²⁴⁹

For publications, apps, and other communicative devices that are incorporated into large schemes to defraud the public and create direct harm, this standard, while stringent, should not be impossible to meet. Where regulators cannot meet it, then the misinformation and negligently fact-checked content must be countered with accurate speech rather than chilling the marketplace of ideas. The First Amendment must allow a good deal of inaccuracy, but it need not immunize intentional harms and the courts and regulators must neither overstate nor understate the scope of unprotected speech when trying to find this balance.

Still, while it seems self-evident that law enforcement and regulatory regimes should be free to stop disinformation, time will tell whether this power will be available to the FTC and to other state and federal regulators.

VI. REGULATING THE USER EXPERIENCE

In addition to enhanced efforts to protect from the false information being promulgated through intentional disinformation, the FTC and states’ attorneys general need to take much stronger action to protect the public from what has become a malevolent user experience in web and app design. The malevolence manifests as a result of the lax privacy and security standards that lag far below that of HIPAA-regulated health care activities, the use of dark patterns, to manipulate consumer responses to mandatory disclosures and user choices, and the aggregation of personal information into consumer scoring and reporting.²⁵⁰ Although the FTC has broad authority, the agency has made clear that it is stepping up

246. *Dongguk Univ. v. Yale Univ.*, 873 F. Supp. 2d 460, 466 (D. Conn. 2012) (citing *DiBella v. Hopkins*, 403 F.3d 102, 110 (2d Cir. 2005) (“The ‘convincing clarity’ by which Sullivan held actual malice must be proved was subsequently interpreted to be synonymous with the more familiar ‘clear and convincing evidence’ standard of proof.”), *aff’d*, 734 F.3d 113 (2d Cir. 2013)).

247. *Ragbir v. Holder*, 389 Fed. App’x. 80, 84–85 (2d Cir. 2010) (unpublished) (quoting *Clear and Convincing Evidence*, BLACK’S LAW DICTIONARY (9th ed. 2009)).

248. *St. Amant v. Thompson*, 390 U.S. 727, 731 (1968).

249. *Garrison v. Louisiana*, 379 U.S. 64, 74 (1964).

250. *See infra* Section II.

antitrust enforcement goals²⁵¹ which leaves the state of consumer protection at largely the status quo.²⁵² Despite the FTC's commitment to protecting the public from unfair and deceptive trade practices,²⁵³ the agency's strategic plan is merely descriptive of the services provided and has little in the form of meaningful new initiatives.

More hopefully, the FTC has begun an Advance Notice of Proposed Rulemaking ("ANPR") regarding the commercial surveillance and data security.²⁵⁴ In announcing the ANPR, FTC Chair Lina Khan stated that:

Today's action marks the beginning of the rulemaking proceeding. In issuing an [ANPR], the Commission is seeking comments from the public on the extent and effects of various commercial surveillance and data security practices, as well as on various approaches to crafting rules to govern these practices and the attendant tradeoffs.²⁵⁵

The ANPR identifies five key concerns regarding the need to switch from a consent model of disclosure to a "minimum necessary" model of disclosure given that most consent is not meaningfully obtained; improved data minimization and similar operational administrability; eliminating discriminatory practices; and addressing the business model of trading privacy for services.²⁵⁶ Each of these five topics is considerable in scope and the ANPR is only a preliminary step. In addition, assuming the rule making is successful, there will need to be significant

251. *See, e.g.*, FED. TRADE COMM'N, RES. DIRECTING USE OF COMPULSORY PROCESS REGARDING ACTS OR PRACTICES RELATED TO TECHNOLOGY PLATFORMS (2021), https://www.ftc.gov/system/files/ftc_gov/pdf/p210100_omnibus_resolution_technology_platforms.pdf [<https://perma.cc/RAD5-54X5>]; FED. TRADE COMM'N, RES. DIRECTING USE OF COMPULSORY PROCESS RE: PROPOSED MERGERS, ACQUISITIONS, AND TRANSACTIONS SUBJECT TO PREMERGER (2021), https://www.ftc.gov/system/files/ftc_gov/pdf/p210100_omnibus_resolution_premerger_transactions.pdf [<https://perma.cc/A65S-HWZL>]. *See also* *FTC Restores Rigorous Enforcement of Law Banning Unfair Methods of Competition*, FED. TRADE COMM'N (Nov. 10, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P221202Section5PolicyStatement.pdf [<https://perma.cc/5WSS-6VNU>].

252. *But see* FED. TRADE COMM'N, STRATEGIC PLAN FOR FISCAL YEARS 2022 TO 2026, https://www.ftc.gov/system/files/ftc_gov/pdf/fy-2022-2026-ftc-strategic-plan.pdf [<https://perma.cc/7VJF-Q3RA>] ("The FTC focuses on investigating and litigating conduct that causes or is likely to cause substantial injury to the public. This includes not only monetary injury, but also, for example, unwarranted health, safety, and privacy risks.")

253. *See id.*

254. *See* Advanced Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 63,738 [hereinafter ANPR]; Lina M. Khan, *Statement of Chair Khan Regarding the Commercial Surveillance Data Security Advance Notice of Proposed Rulemaking*, FTC (Aug. 11, 2022), <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-chair-khan-regarding-commercial-surveillance-data-security-advance-notice-proposed> [<https://perma.cc/3G3F-EGUR>] [hereinafter ANPR Statement].

255. Khan, ANPR Statement, *supra* note 249, at 3.

256. *See id.*

congressional funding support to turn these additional rules into an enforceable new regulatory regime.

The FTC is not alone in trying to take new steps to increase legal protections for data privacy, information security, and in reducing consumer manipulation. Congress itself has taken significant steps towards the first comprehensive U.S. privacy law. “On July 20, 2022, the House Energy and Commerce Committee voted 53-2 to advance the American Data Privacy and Protection Act (ADPPA), H.R. 8152, to the full House of Representatives.”²⁵⁷ The proposal offered a model of aggressive privacy protection, increased protection for minors, and limited private rights of action.²⁵⁸

Unfortunately, the lobby that has enacted California’s state privacy legislation is opposed to the adoption of a national standard that could preempt state law. As a result, the legislation remains in limbo.²⁵⁹ Even if passed, the mandatory provisions would likely face close constitutional scrutiny under recent Supreme Court decisions under commercial speech doctrine.²⁶⁰ The same factors that have made the court treat commercial regulations of advertising and disclosures could potentially threaten efforts to limit what companies can do to collect or disseminate consumer information.²⁶¹

Even more than the general restrictions the Supreme Court has been placing on commercial speech regulation, the newly discovered “major questions doctrine” threatens to usurp executive power by the judiciary. “Under this body of law, known as the major questions doctrine, given both separation of powers principles and a practical understanding of legislative intent, the agency must point to clear congressional authorization for the authority it claims.”²⁶² The major questions doctrine, combined with the commercial speech concerns about viewpoint

257. Overview of the American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022), <https://crsreports.congress.gov/product/pdf/LSB/LSB10776> [<https://perma.cc/FJ63-EGJV>].

258. *See id.* (“The ADPPA would create a comprehensive federal consumer privacy framework. Some commentators have noted the bill’s novel compromises on two issues that have impeded previous attempts to create a national privacy framework: whether to preempt state privacy laws and whether to create a private right of action.”).

259. Cameron F. Kerry, *Will California be the death of national privacy legislation?*, BROOKINGS (Nov. 18, 2022), <https://www.brookings.edu/blog/techtank/2022/11/18/will-california-be-the-death-of-national-privacy-legislation/> [<https://perma.cc/FG2C-JGDF>].

260. *E.g.*, *Barr v. Am. Ass’n of Pol. Consultants*, 140 S. Ct. 2335 (2020) (plurality); *Iancu v. Brunetti*, 139 S. Ct. 2294 (2019); *Reed v. Gilbert*, 135 S. Ct. 2218 (2015); *Sorrell v. IMS Health*, 564 U.S. 552 (2011). *See infra* note 255 and accompanying text on shift in commercial speech doctrine.

261. *See id.* *See also* *West Virginia v. EPA*, 142 S. Ct. 2587 (2022).

262. *West Virginia*, 142 S. Ct. at 2595.

discrimination, will make any regulations much more difficult to enforce under Section 5 of the FTC Act or under newly enacted federal law.

Still, for the health care sector, there might be some residual authority even if the Supreme Court interferes with more general commercial regulation. In most instances, the Supreme Court has continued to permit Congress to include eligibility restrictions for federal funds on limited speech restrictions.²⁶³ If Congress finds itself thwarted in efforts to expand privacy protections under the First Amendment, it can tie additional privacy protections to non-HIPAA entities that receive funding through federal grants or contracts to undertake an additional set of privacy and cybersecurity protections that enhance security and prohibit data aggregation and scoring of consumers.

VII. RECLAIMING THE MARKETPLACE OF HEALTH INFORMATION FROM DISINFORMATION

However, even assuming that new legislation emboldens the FTC and a shift in the Supreme Court jurisprudence on commercial speech, health care outcomes are likely to continue to be harmed by the pervasive efforts of hackers, hucksters, amoral corporate practices, and belligerent foreign nations. Enforcement actions simply cannot keep up with the data theft and disinformation campaigns. So long as Fortune 500 companies continue to use dark patterns in their marketing with impunity, the public will continue to be harmed. In addition, the marketplace remains vulnerable to the negligently inaccurate content and the content promulgated and shared with a willful blindness designed to avoid falling afoul of the knowing disinformation standard. Regulation alone is simply insufficient, no matter how essential it may be.

As a consequence, the public health advocates need a different alternative. They need to nudge the public to better health, but more than merely nudge, they need to take advantage of the behavioral economics lessons to promote good public health outcomes aggressively and discourage—but not ban—negative health outcomes. Historically, “although health professionals use the media widely for health promotion,

263. *Rust v. Sullivan*, 500 U.S. 173 (1991) (upholding health care service restrictions on counseling regarding abortion services). *See United States v. Am. Libr. Ass’n., Inc.*, 539 U.S. 194 (2003) (upholding the constitutionality of requiring that public libraries install anti-indecency filters on internet-enabled computers as a condition of receiving low cost internet provided in the E-rate program established by the Telecommunications Act of 1996, 110 Stat. 71, 47 U.S.C. § 254(h)(1)(B) and mandated as a condition for receiving grants under the Library Services and Technology Act (LSTA), 20 U.S.C. § 9101).

they do so mainly to ‘advertise’ health products or programs and not to motivate behavior change.”²⁶⁴

It is unclear the extent to which the use of mass media and social media have changed in the information age. At least the significance of outreach has grown. “Communication is a key part of the practice of public health and is a core competency required to be taught by schools of public health across the United States.”²⁶⁵ It needs to become a public mandate.

The COVID-19 Pandemic provides a snapshot of the way in which public health organizations were overwhelmed. For example, a report from the Pan American Health Organization in association with the World Health Organization (“WHO”) describes a single 30-day period during the pandemic:

361,000,000 videos were uploaded on YouTube in the last 30 days under the “COVID-19” and “COVID 19” classification, and about 19,200 articles have been published in Google Scholar since the pandemic started. In the month of March, around 550 million tweets included the terms coronavirus, corona virus, covid19, covid-19, covid_19, or pandemic.²⁶⁶

In contrast to this overwhelming production of content, the WHO employs “[a]bout 20 staff and some consultants are involved in WHO’s communications teams globally, at any given time.”²⁶⁷ These personnel include communications consultants and communications officers stationed throughout six different WHO offices.²⁶⁸ Their role is to connect with media platforms, presumably to promote content regulation policies that encourage the promotion of accurate information and to encourage companies to be more active in their content moderation.²⁶⁹

Of course, each government has its own information bureau. In the United States, this includes governmental agencies at both the federal and state levels. Every public hospital and every research university has the

264. Laurie Hoffman-Goetz & Sandra Dwiggin, *Teaching Public Health Practitioners About Health Communication: The MPH Curriculum Experience*, 23 J. CMTY. HEALTH 127, 128 (1998).

265. Megan L. Ranney & Stefanie Friedhoff, *Public communication about public health where we really need to go*, 5 NPJ DIGIT. MED. 28 (Mar. 8, 2022). See *Accreditation Criteria Schools Of Public Health & Public Health Programs*, COUNCIL ON EDUC. FOR PUB. HEALTH (Aug. 2021), <https://media.ceph.org/documents/2021.Criteria.pdf> [<https://perma.cc/M6PX-HKX7>].

266. *Understanding the Infodemic and Misinformation in the fight against COVID-19*, PAN AM. HEALTH ORG. (last visited Nov. 22, 2022), <https://iris.paho.org/handle/10665.2/52052> [<https://perma.cc/HN7L-7JFN>].

267. John Zarocostas, *How to fight an infodemic*, 395 LANCET, Feb. 29, 2020, at 1.

268. *Id.*

269. *See id.*

ability to produce its own content as well. But as noted at the beginning of the article, the majority of content being produced was not coming from these reputable sources and the majority of Covid information was simply inaccurate. Nor is this phenomenon limited to the Covid outbreak.²⁷⁰

While individual health outcomes might be subject to a myriad of variables, the New York City Commissioner of Health remarked in 1914 that “public health is purchasable.”²⁷¹ This observation reflects that “a community’s or a nation’s inhabitants (or their elected representatives) will decide their health status by how they allocate funding.”²⁷² In the United States, the funding is not well used. “The United States spends more than other countries without obtaining better health outcomes.”²⁷³ Perhaps the money should be redirected.

In the United States, “public health” represents only 2.5²⁷⁴ to 3.1 percent of total health spending.²⁷⁵ Public health spending is generally defined to include “epidemiologic surveillance, immunization, and vaccination, disease prevention programs, public health laboratories, and similar population-based health services.”²⁷⁶ The data collected, however, varies in its categorizations and definitions. Nonetheless, the picture that emerges is clear. Despite an overall spending of \$4.1 trillion on health care in 2020,²⁷⁷ only a fraction is spent on prevention and the amount spent on public education is so trivial as not to be measured.²⁷⁸

270. See Desai et al., *supra* note 99 and accompanying text.

271. COMM. ON PUB. HEALTH STRATEGIES TO IMPROVE HEALTH; INST. MED., FOR THE PUBLIC’S HEALTH: INVESTING IN A HEALTHIER FUTURE 101 (2012) (quoting New York City’s Commissioner of Health Herman M. Biggs who added that “within natural limitations, a community can determine its own death rate.”).

272. *Id.*

273. Ryan Nunn, Jana Parsons & Jay Shambaugh, *A dozen facts about the economics of the US health-care system*, BROOKINGS (March 10, 2020), <https://www.brookings.edu/research/a-dozen-facts-about-the-economics-of-the-u-s-health-care-system/> [<https://perma.cc/N3SW-WWSX>].

274. *The American Public Health Association strongly supports the Prevention and Public Health Fund, a critical investment that is integral to addressing the burden of chronic and preventable disease in the United States*, AM. PUB. HEALTH ASS’N 1, https://www.apha.org/-/media/files/pdf/factsheets/200129_pphf_factsheet.ashx [<https://perma.cc/4YPP-YRZH>].

275. COMM. ON PUB. HEALTH STRATEGIES TO IMPROVE HEALTH, *supra* note 266, at 104 (“In 2009, according to [the Centers for Medicare and Medicaid Services (CMS) Office of the Actuary National Health Expenditure Accounts (NHEA)], 3.1 percent of the nation’s nearly \$2.5 trillion spent on health, or \$77.2 billion, was spent on government public health activities.”).

276. *Id.* at 102–03.

277. *National Health Spending in 2020 Increases due to Impact of COVID-19 Pandemic*, CTRS. FOR MEDICARE & MEDICAID SERVS. (Dec. 15, 2021), <https://www.cms.gov/newsroom/press-releases/national-health-spending-2020-increases-due-impact-covid-19-pandemic> [<https://perma.cc/3KDN-D65C>] (“[T]he COVID-19 pandemic had a dramatic impact on the nation’s health sector in 2020, driving a 9.7% growth in total national healthcare spending, bringing spending to \$4.1 trillion.”).

278. See COMM. ON PUB. HEALTH STRATEGIES TO IMPROVE HEALTH, *supra* note 266, at 104.

It stands to reason that a criminal enterprise which hopes to maximize wealth while minimizing risk would attack the public health system. Regulators are leery of addressing the “content” of these malefactors, the public is hungry for information, particularly in times of crisis, and the official government speech is all but invisible.

During the pandemic, the most notable exception was the independent and highly articulate voice of Dr. Anthony Fauci.²⁷⁹ By the middle of 2020, he was famous. “Pandemic-memorabilia entrepreneurs have put his face on bottle openers, coffee mugs, and bumper stickers: ‘In Dr. Fauci we trust.’ The National Bobblehead Hall of Fame and Museum has produced a seven-inch likeness of him, partly to raise money to produce protective gear for medical workers.”²⁸⁰

The rise of “In Dr. Fauci we trust,” is not a testament to his personal success, however, so much as an indicator of the void into which he was thrust. The United States does not fund or operate a communications network that connects in health care infrastructure to promote wellness in normal times and could not pivot to crisis mode to address these concerns.

This is a national failure that costs lives and leaves the marketplace to those that would harm the public. If the best medicine for bad speech is the disinfectant of accurate speech, then that speech needs to be produced in volume. In 2020, the combination of Medicare and Medicaid exceeded \$1.5 trillion.²⁸¹ One percent of this funding would provide more than \$15 billion dollars in funding of communications and communications infrastructure, but even a quarter of that could fundamentally change health outcomes and public behavior.

The Centers for Disease Control has received significant additional funding in the past two years and has been investing in public health infrastructure. But while this is an essential part of the public health strategy, the plans do not seem to include public education.²⁸² Without funding public education and training the public to create and disseminate accurate public information, the efforts to improve health outcomes will continue to be drowned out in the marketplace.

279. See Michael Specter, *How Anthony Fauci Became America’s Doctor*, THE NEW YORKER (April 10, 2020) <https://www.newyorker.com/magazine/2020/04/20/how-anthony-fauci-became-americas-doctor> [<https://perma.cc/Y9DD-FJXS>].

280. *Id.* (“These days, nearly everyone has heard of Fauci.”).

281. *National Health Spending in 2020*, *supra* note 272 (Medicare spending totaled \$829.5 billion in 2020, and Medicaid spending increased to \$671.2 billion—for a total of \$1500.7 trillion).

282. See, e.g., *CDC to Invest \$2.1 Billion to Protect Patients and Healthcare Workers from COVID-19 and Future Infectious Diseases*, CTRS. FOR DISEASE CONTROL AND PREVENTION (Sept. 17, 2021), <https://www.cdc.gov/media/releases/2021/p0917-COVID-19-funding.html> [<https://perma.cc/J2YH-L627>] (listing uses of a \$2.1 billion funding).

Funding public health information makes good economic sense as well. Studies have consistently shown that such campaigns provide a positive return on investment because the reduced need for health services is significantly greater than the cost of the information.²⁸³ When used, health information programs have a “typical return on investment” at twice the rate of expenditure.²⁸⁴ With improvement to the manner in which these campaigns are designed, the impact can likely be increased even further.

Public health communication is a foundational domain for a bachelor’s degree in Public Health, involving “basic concepts of public health-specific communication, including technical and professional writing and the use of mass media and electronic technology.”²⁸⁵

More than twenty years ago public health educators recognized the potential of the new media to transform public health.²⁸⁶ “Health communications transforms scientific recommendations into message strategies relevant to the consumer—however that consumer is defined. Health information systems and health communications, then, are the ties that bind the disciplines of public health, health services, and clinical medicine.”²⁸⁷ With the rise of social media and the cusp of the metaverse, these demands are even more pressing.

Though new social media channels and terminology have emerged relatively recently in the public health communication area, engagement is not a new concept. . . . Public health defines *community engagement* as “the process of working collaboratively with and through groups of people affiliated by geographic proximity, special interest, or similar situations to address issues affecting the well-being of those people.” Similarly, *community building* . . . is “an orientation to the ways in

283. See Aaron E. Carroll & Austin Frakt, *It Saves Lives. It Can Save Money. So Why Aren't We Spending More on Public Health?*, N.Y. TIMES (May 28, 2018), <https://www.nytimes.com/2018/05/28/upshot/it-saves-lives-it-can-save-money-so-why-arent-we-spending-more-on-public-health.html> [<https://perma.cc/STD5-86N2>].

284. *Id.* (“Health promotion interventions, including programs to prevent falls among older people or campaigns to get people to quit smoking, have a typical return on investment of only 2. Returns can be higher if programs perform better at targeting high-risk people.”).

285. Accreditation Criteria, *supra* note 260, at 27–28.

286. See Richard Riegelman & Nancy Alfred Persily, *Health information systems and health communications: Narrowband and broadband technologies as core public health competencies*, 91 AM. J. PUB. HEALTH 1179 (Aug 2001).

287. *Id.* (“Health communications represents an unprecedented potential for getting the word out, using print and broadcast media and disseminating positive messages through movies, sitcoms, soap operas, and even MTV.”)

which people who identify as members of a shared community engage together in the process of community change.”²⁸⁸

Communication is the art of being heard and understood rather than merely the mechanics of delivery. Public health communication, therefore, must be mediated in a manner that takes the communities for whom the information is provided into account when offering those services.²⁸⁹ In this regard, public health information must be designed to provide the most appropriate messages and reconceived to provide visually impactful information.²⁹⁰ “The ‘new communication’ and ‘new language’ of the visual design already present in emerging media, as well as an in-depth examination of new modes of expression and particular applications in emerging media, should be the focus of visual transmission design under emerging media technology.”²⁹¹

The communications design cannot be afraid to nudge the public to make healthy choices and overcome the sludge and dark patterns used by industry. Clinical trials show these techniques work. “Nudges, defined as interventions that alter ‘people’s behavior in a predictable way without forbidding any options or significantly changing economic incentives,’ . . . have been effectively applied to . . . health-related decisions, such as healthy eating, exercising and influenza vaccinations.”²⁹² The trials worked for COVID-19 as well. “Nudges . . . could improve the uptake of COVID-19 vaccines Our research highlights that behavioural science insights can increase and speed up COVID-19 vaccinations at close-to-zero marginal cost.”²⁹³ Behavioral science has become an intrinsic aspect of commercial

288. Amy B. Heldman, Jessica Schindelar & James B. Weaver, *Social Media Engagement and Public Health Communication: Implications for Public Health Organizations Being Truly “Social,”* 35 PUB. HEALTH REVS. 1, 5 (2013) (first quoting CLINICAL AND TRANSLATIONAL SCIENCE AWARDS CONSORTIUM COMMUNITY ENGAGEMENT KEY FUNCTION COMMITTEE TASK FORCE ON THE PRINCIPLES OF COMMUNITY ENGAGEMENT, PRINCIPLES OF COMMUNITY ENGAGEMENT (2d ed. 2011), http://www.atsdr.cdc.gov/communityengagement/pdf/PCE_Report_508_FINAL.pdf [<https://perma.cc/YJU7-YQZQ>]), then quoting Meredith MINKLER, NINA WALLERSTEIN & NANCE WILSON, HEALTH BEHAVIOR AND HEALTH EDUCATION: THEORY, RESEARCH, AND PRACTICE 279–311 (Glanz K, Rimer BK, Lewis FM eds., 3d ed., Josey-Bass 2002)).

289. *See id.* at 5–8.

290. *See* Ke Wang & Caiyuan Kuang, *Visual Communication Design Model for New Media and Public Health Environment and New Communication Mode*, 2022 J. OF ENV’T & PUB. HEALTH 1 (2022).

291. *Id.*

292. Hengchen Dai, Silvia Saccardo, Maria A. Han, Lily Roh, Naveen Raja, Sitaram Vangala, Hardikkumar Modi, Shital Pandya, Michael Sloyan & Daniel M. Croymans, *Behavioural nudges increase COVID-19 vaccinations*, 597 NATURE 404, 404 (2021).

293. *Id.*

marketing, and it needs to be utilized throughout the public health communications systems to achieve public health benefits.

In addition, as a side benefit, the work to improve public health communications education and application will improve the digital literacy of the personnel trained in the communications.²⁹⁴ With funding and an emphasis on overcoming the sludge and dark patterns, professional communicators in the health and wellness fields would have a broader public benefit. They would be able to promote digital literacy, which is a foundational aspect of education for public citizenship.²⁹⁵ The concerted effort to respond to the sludge and dark patterns of the sickness industries, the addiction industries, and the profiteers on misery cannot be stopped with a PSA. It will take an industry of professionals who understand the best in communication strategy and behavioral economics combined with the health and wellness knowledge to promote accurate health information in order to assist the public in making informed, healthy choices.

Without this effort, the next health crisis will look exactly like the last one as will each one that follows. Without changing public behavior to these crises, the exploitation and disinformation will only grow with each iteration. With a proper investment, the cycle can be disrupted. That disruption will not come from a more muscular FTC alone; that disruption can only be truly successful by taking back the information marketplace itself.

VIII. CONCLUSION

The Supreme Court has shifted the legal protection for commercial speech from its content-based balancing test in *Central Hudson* to an increasingly content-neutral requirement for regulation. But, as discussed above, that does not mean the government has lost its power to proscribe and punish fraudulent, harmful, or knowingly false speech. The FTC had done so for over a century and will continue to do so in the future. But as the amount of misinformation and disinformation in the health

294. See, e.g., *Certified Health Education Specialist*, NAT'L COMM'N FOR HEALTH EDUC. CREDENTIALING, <https://www.nchec.org/> [<https://perma.cc/99MR-S4V7>]; *Master of Science in Public Health (MSPH) in Health Education and Health Communication*, JOHNS HOPKINS UNIV., DEPT. OF HEALTH, BEHAVIOR AND SOC'Y, <https://publichealth.jhu.edu/academics/msph-in-health-education-and-health-communication> [<https://perma.cc/Y6SA-UWZT>].

295. See Romina Bandura & Elena I. Méndez Leal, *The Digital Literacy Imperative*, CTR FOR STRATEGIC AND INT'L STUDS. (July 18, 2022), <https://www.csis.org/analysis/digital-literacy-imperative> [<https://perma.cc/GZ6D-7UC3>]. See generally, JON M. GARON, PARENTING FOR THE DIGITAL GENERATION (ROWMAN & LITTLEFIELD 2021).

information sector grows, expanding the role for the FTC is essential but not sufficient.

The essential requirement is that the FTC not concede its authority to address unfair and deceptive practices that occur throughout the health information distribution network. Nothing in the law requires that the FTC limit itself to advertising and any content that meets the actual malice standard is outside of First Amendment protection and should be stopped if it is materially harmful to the public.

Nonetheless, the FTC is the backstop to a working marketplace. At present, the marketplace for health information is dominated by those who create content for the purposes of profit—often at a high cost to public health. To meet this threat, the government must meaningfully fund public health information with sufficient resources to overcome the existing public health disinformation industry to provide accurate, timely, and behaviorally motivating information to the public in order to save lives and promote better health.

Public health spending is at an all-time high and growing. Still, for millions of people, the available advice is wildly inaccurate, produced only to sell the snake oil of the promoter. The false claims offer unhelpful and often unhealthy advice. They stop the public from receiving proper treatment. The hucksters fuel their disinformation with sludge and dark patterns informed and shaped by health information acquired from the unregulated marketplace or stolen data purchased from hackers. Although new technologies provide opportunities for greater access to information and better-informed treatment strategies, the disinformation and sludge excludes millions of individuals from these benefits.

The government has the authority and resources to reclaim the public health marketplace. To do so will simply take political will. Professionals must be trained, and institutions resourced to provide accurate, timely, informative, and persuasive information to promote public health and positive health choices. It will be expensive, but it will pay for itself and likely generate net reductions in overall health expenditures. The government has a duty to protect its citizens and a democratic society prioritizes the autonomy of its citizens to make their own choices. Police power is neither optimal to solve the problem nor practical. Yet something must be done. The answer must therefore be to educate and to do so with the same level of investment as those who seek to profit on the disinformation. Nothing less will suffice.