Printed in U.S.A.
Vol. 115, No. 6

INFORMATION FIDUCIARIES AND POLITICAL MICROTARGETING: A LEGAL FRAMEWORK FOR REGULATING POLITICAL ADVERTISING ON DIGITAL PLATFORMS

Kimberly Rhum

ABSTRACT—Digital technologies have taken individualized advertising to an unprecedented level. But the convenience and efficiency of such highly tailored content comes at a high price: unbridled access to our personal data. The rise of sophisticated data-driven practices, otherwise known as "Big Data," enables large datasets to be analyzed in ways that reveal useful patterns about human behavior. Thanks to these novel analytical techniques, businesses can cater to individual consumer needs better than ever before. Yet the opportunities presented by Big Data pose new ethical challenges.

Significant scholarly research has examined algorithmic discrimination and consumer manipulation, as well as the ways that data-driven practices undermine our democratic system by dramatically altering the news ecosystem. Current scholarship has especially focused on the ways illegitimate foreign and domestic operatives exploit the advertising tools of digital platforms to spread fake and divisive messages to those most susceptible to influence. However, more scholarly attention should be devoted to how these digital technologies are exploited by legitimate political actors, such as politicians and campaigns, to win elections.

By combining data-driven voter research with personalized advertising, political actors engage in political microtargeting, directing communications at niche audiences. Political microtargeting fits within a broader conversation about data-privacy regulation, as individuals lack sufficient control over how digital companies handle their personal data. The First Amendment currently limits data-privacy reform, so any meaningful changes must reconcile data privacy with the First Amendment.

Professor Jack Balkin has argued that online service providers should be defined as "information fiduciaries," or businesses that, because of their relationship with another, have taken on special duties with respect to the information they obtain in the course of the relationship. Because online service providers receive sensitive information from their end users, Professor Balkin argues they should be subject to additional regulation. Treating online service providers as information fiduciaries provides a viable

means to reconcile the First Amendment with data-privacy regulation: the First Amendment has not prevented the state or federal government from regulating how certain professionals, such as doctors and lawyers, interact with their clients and use their personal information because these professionals share a fiduciary relationship with their clients. Therefore, consistent with the First Amendment, the government should also be able to subject online service providers to reasonable restrictions on their handling of end-user data.

This Note expands Professor Balkin's information-fiduciary framework by arguing that federal legislation should place fiduciary duties on online service providers. In doing so, it responds to scholarly critiques of Professor Balkin's theory, particularly the criticism that he failed to show how information fiduciaries might function in practice. Using political microtargeting on Facebook as an example, this Note spells out the ways that fiduciary duties might be enforced. This Note argues that holding Facebook and other digital platforms that engage in political advertising to an information-fiduciary standard would ameliorate some of the adverse effects of political microtargeting and promote electoral integrity in the digital age.

AUTHOR—J.D. Candidate, Northwestern Pritzker School of Law, 2021; B.A., Northwestern University, 2018.

INTRODUCTION

In today's digital landscape, personalization is the name of the game.[1] From the food we eat, to the shows we watch, to the music we stream, to even the people we date, digital technologies have taken individualized advertising to an unprecedented level,[2] drastically transforming the choices we make in our everyday lives.[3] Craving a cheeseburger and fries from the comfort of your home? Here's a list of the ten closest hamburger joints available for delivery, courtesy of Uber Eats.[4] Finished with *Friends* and in desperate search of a new comedy series to binge-watch? Netflix has got you covered with a list of related shows that fit your viewing needs.[5] Dreading that long commute to work? Spotify's "Made For You" service combines all your favorite tunes in one place,[6] making your daily commute a little bit more bearable. Ready to settle down and find that special someone? Match.com has got your perfect match.[7] While modern digital technologies bring endless possibilities for optimizing the user experience, the convenience and efficiency of such highly tailored content comes at a crucial price: unbridled access to our personal data.[8]

---

[1] *See, e.g.*, Nik Spirin, *An Overview of Personalization Technologies Across the Internet*, MEDIUM (Feb. 27, 2018), https://medium.com/technology-insights/an-overview-of-personalization-technologies-across-the-internet-c641299abfab [https://perma.cc/74U6-PYHN] ("Personalization [is] at the core of many modern internet services . . . ."); Shayna Hodkin, *The Internet of Me: Creating a Personalized Web Experience*, WIRED (Nov. 21, 2014), https://www.wired.com/insights/2014/11/the-internet-of-me [https://perma.cc/6RBE-HYBV] ("The Internet you experience is as unique to you as your fingerprint.").

[2] *See* Amanda Zantal-Wiener, *These 9 Brands Take Personalized Marketing to a New Level*, HUBSPOT (June 1, 2020), https://blog.hubspot.com/marketing/marketing-personalization-examples [https://perma.cc/LK48-L3JV] (illustrating how specific brands have offered a "personalized and meaningful marketing experience" in a way that is not overly intrusive).

[3] ELI PARISER, THE FILTER BUBBLE: WHAT THE INTERNET IS HIDING FROM YOU 9 (2011) (describing digital platforms as creating "a unique universe of information" that "fundamentally alters the way we encounter ideas and information").

[4] *See generally How Uber Eats Works*, UBER EATS, https://about.ubereats.com [https://perma.cc/3822-RXAM] (informing customers generally about what they can browse and how they can order through Uber Eats).

[5] *See How Netflix's Recommendations System Works*, NETFLIX, https://help.netflix.com/en/node/100639 [https://perma.cc/EY8P-UZFA].

[6] *See Made for You*, SPOTIFY, https://support.spotify.com/us/article/made-for-you-playlists [https://perma.cc/7EVS-8B74].

[7] *See About Match.com*, MATCH, https://www.match.com/help/aboutus.aspx?lid=4 [https://perma.cc/EHZ6-ZF3H].

[8] *See* SAM MACBETH, CLIQZ, TRACKING THE TRACKERS: ANALYSING THE GLOBAL TRACKING LANDSCAPE WITH GHOSTRANK 13 (2017), https://cdn.cliqz.com/wp-content/uploads/2017/12/Ghostery_Study_-_Tracking_the_Trackers.pdf [https://perma.cc/624Z-HUAQ] (finding that Google and Facebook track "64% and 29% of pages loaded on the web," respectively); *see also* James Pasley, *28 Ways Companies and Governments Can Collect Your Personal Data and Invade Your Privacy Every Day*, BUS. INSIDER (Jan. 21, 2020, 9:42 AM), https://www.businessinsider.com/invasion-of-data-

Our personal data is the oil fueling today's digital economy.[9] The term "personal data" refers to personally identifiable information that can be linked to a specific individual.[10] Whether making purchases at a store, eating at a restaurant, shopping for a car, or surfing the web, consumers engage in activities on a daily basis that reveal valuable personal information about them.[11] There are three main ways that companies can collect personal data: ask their customers directly for it,[12] indirectly track them,[13] or acquire the data from other entities.[14] The rise of sophisticated, data-driven practices, otherwise known as "Big Data,"[15] enables large datasets to be analyzed in

privacy-online-in-person-examples-2020-1 [https://perma.cc/3M7L-SSZP] ("In modern life, privacy is relinquished in so many ways—from your daily commute, to how productive you are at work, to what you search on Google, to what you buy in a store.").

[9] Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who Is Using It)*, WIRED (Feb. 15, 2019, 7:00 AM), https://www.wired.com/story/wired-guide-personal-data-collection [https://perma.cc/6CCS-LWRC] ("Personal data is often compared to oil—it powers today's most profitable corporations, just like fossil fuels energized those of the past.").

[10] *What Is Personal Data?*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data [https://perma.cc/Y6H4-Y6BS]. Personal data may include anything from "[s]ocial media posts, location data, and search-engine queries" to more sensitive information such as "[h]ealth records, social security numbers, and banking details." Matsakis, *supra* note 9.

[11] *See Sharing Information: A Day in Your Life*, FTC, http://www.consumer.ftc.gov/media/video-0022-sharing-information-day-your-life [https://perma.cc/LU6V-JD94].

[12] When a customer subscribes to a service or buys something online for the first time, a company will likely ask for a name and email address. Customer surveys are another way to directly ask for data from consumers. William Goddard, *How Do Big Companies Collect Customer Data?*, IT CHRONS. (Jan. 14, 2019), https://itchronicles.com/big-data/how-do-big-companies-collect-customer-data [https://perma.cc/9QD3-ZF6Q].

[13] Companies can also obtain customer data through online trackers. Websites may be equipped with cookies that inform companies about what customers have looked at online and where they go after they've finished browsing the company's site. This cross-site tracking function explains why when you look at a pair of sneakers on a website, you will frequently find an ad for the same sneakers following you around the web. *See id.* Furthermore, apps such as Uber, Snapchat, Spotify, and Tinder are embedded with third-party "trackers" that provide customer data used "for targeted advertising, behavioral analytics, and location tracking." *See ISP Privacy Lab Publishes Research on Hidden Trackers*, YALE L. SCH. (Nov. 28, 2017), https://law.yale.edu/yls-today/news/isp-privacy-lab-publishes-research-hidden-trackers [https://perma.cc/U5LT-ELUA].

[14] Third-party companies known as data brokers exist for the sole purpose of collecting, analyzing, and selling data to companies for targeted advertising campaigns. Data brokers collect data from commercial, government, and other publicly available sources. *See* FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 3 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/SSA5-WFGY].

[15] Jenifer Winter, *Algorithmic Discrimination: Big Data Analytics and the Future of the Internet*, *in* THE FUTURE INTERNET: ALTERNATIVE VISIONS 125, 128 (Jenifer Winter & Ryota Ono eds., 2015) (defining "Big Data" as "the term used to describe large, complex data sets that require novel data management tools").

ways that reveal useful patterns about human behavior.[16] "Big Data is crucial to the . . . development of algorithms and artificial intelligence" (AI), which companies rely upon to classify and make decisions about consumers.[17] Thanks to these new analytical techniques, businesses are able to cater to individual consumer needs better than ever before.[18]

But the opportunities presented by Big Data also pose new ethical challenges. Businesses might offer different products, services, or prices to consumers based on their data profiles, giving rise to "algorithmic discrimination"—the presence of bias within computer systems that creates unfair or discriminatory outcomes.[19] Algorithmic discrimination has already sparked lawsuits[20] and led to proposed legislation requiring companies to evaluate their algorithms for impacts on accuracy, discrimination, privacy, and security.[21]

Furthermore, Big Data offers a unique window into consumer psychology, as sophisticated prediction algorithms not only analyze individual behaviors, but also make inferences about intimate psychological traits, such as personality, IQ, and political orientation.[22] While

---

[16] *What Is Big Data?*, ORACLE, https://www.oracle.com/big-data/what-is-big-data.html [https://perma.cc/W8JT-NWD6] ("Put simply, big data is larger, more complex data sets . . . . [that] can be used to address business problems you wouldn't have been able to tackle before.").

[17] Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1154, 1156 (2018).

[18] *See, e.g.*, Frank van den Driest, Stan Sthanunathan & Keith Weed, *Building an Insights Engine*, 94 HARV. BUS. REV. 64, 66 (2016) (describing how a customer-centric approach serves as a powerful source of competitive advantage in the Big Data era).

[19] Winter, *supra* note 15, at 131 ("[Big Data] exposes sensitive behaviors or other personal information that could be used to disadvantage certain individuals or groups by corporations or governments. For example, citizens may experience political and economic discrimination related to housing, immigration, employment, political, or health-related behaviors." (citation omitted)).

[20] *See, e.g.*, Reed Albergotti, *Group of Black Creators Sue YouTube, Alleging Racial Discrimination*, INDEPENDENT (June 18, 2020, 7:26 PM), https://www.independent.co.uk/news/long_reads/science-and-technology/youtube-black-creators-suing-legal-action-google-nicoles-view-a9573176.html [https://perma.cc/6ESE-UE98] (describing a lawsuit filed against YouTube alleging racial discrimination relating to the platform's systematic removal of content); Ariana Tobin, *HUD Sues Facebook over Housing Discrimination and Says the Company's Algorithms Have Made the Problem Worse*, PROPUBLICA (Mar. 28, 2019, 1:18 PM), https://www.propublica.org/article/hud-sues-facebook-housing-discrimination-advertising-algorithms [https://perma.cc/LHH2-ZWM5] (discussing a lawsuit filed against Facebook alleging housing discrimation related to the company's algorithms).

[21] *See* Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (requiring companies to study and fix flawed computer algorithms that result in inaccurate, biased, or discriminatory decisions affecting Americans).

[22] Sandra C. Matz & Oded Netzer, *Using Big Data as a Window into Consumers' Psychology*, 18 CURRENT OP. BEHAV. SCI. 7, 8 (2017).

psychological targeting can help consumers make better choices,[23] it can also be used to exploit individual vulnerabilities, generating concerns over consumer manipulation.[24] Significant research has centered on the potentially discriminatory effects of algorithm-based decisions[25] and the implications of Big Data on consumer manipulation.[26] Recent scholarship has also examined how these data-driven practices undermine our democratic system by dramatically altering the news ecosystem[27] and the electoral process.[28]

---

[23] Psychologically personalized marketing can alleviate the problem of choice overload, help maximize the happiness consumers gain from their choices, and prove effective in changing behaviors among patients and groups who are at risk. *See, e.g.*, Barry Schwartz & Andrew Ward, *Doing Better but Feeling Worse: The Paradox of Choice*, *in* POSITIVE PSYCHOLOGY IN PRACTICE 86, 97–99 (P. Alex Linley & Stephen Joseph eds., 2004) (discussing the consequences associated with an overabundance of choice, which includes an uptick in clinical depression); Sandra C. Matz, Joe J. Gladstone & David Stillwell, *Money Buys Happiness when Spending Fits Our Personality*, 27 PSYCHOL. SCI. 715, 722 (2016) (finding "that individuals' happiness can be increased through the consumption of products that match [an individual's] psychological chararacteristics").

[24] *See, e.g.*, Brett Abarbanel, Sally M. Gainsbury, Daniel King, Nerilee Hing & Paul H. Delfabbro, *Gambling Games on Social Platforms: How Do Advertisements for Social Casino Games Target Young Adults?*, 9 POL'Y & INTERNET 184, 202–04 (2016) (explaining how advertisements for social gambling games on platforms encourage gambling among youth but are not subject to the same regulations as real-money gambling).

[25] *See, e.g.*, Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 677–93 (2016) (explaining that data-driven analyses often reinforce discrimination against members of protected groups); Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857, 880–81 (2017) (showing that algorithms based on inaccurate or unrepresentative data can lead to discrimination against minority applicants).

[26] *See, e.g.*, Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 996, 999 (2014) (exploring companies' ability to collect data on consumers and the costs associated with how this unduly influences consumer decision-making); Max N. Helveston, *Consumer Protection in the Age of Big Data*, 93 WASH. U. L. REV. 859, 897–98 (2016) ("[W]hen insurers have the ability to influence the behavior of their customers, they will push policyholders to act in ways that do not maximize overall societal utility.").

[27] *See, e.g.*, Martha Minow, *The Changing Ecosystem of News and Challenges for Freedom of the Press*, 64 LOY. L. REV. 499, 500–02 (2018) ("The ecosystem of news has changed beyond the imagination of anyone living when the First Amendment was drafted.").

[28] *See, e.g.*, Matthew Crain & Anthony Nadler, *Political Manipulation and Internet Advertising Infrastructure*, 9 J. INFO. POL'Y 370, 370 (2019) (explaining that "digital advertising infrastructure, as it is currently designed and managed, creates opportunities for political manipulation and foreign interference" in U.S. elections).

Digital platforms such as Facebook,[29] Twitter,[30] and Google,[31] while designed to reach broad audiences, foster community, and propagate the spread of diverse voices and ideas, have instead created digital echo chambers[32] that paradoxically inhibit the online marketplace of ideas.[33] Much like in commercial advertising, personalization has become the norm in the news industry.[34] Today, data-driven algorithms, rather than human editors, determine the news we receive.[35] Yet, the underlying algorithms and digital advertising infrastructure that dictate content visibility remain hidden from public view, creating an imbalance of power and information between digital platforms and their end users of enormous political consequence.[36]

---

[29] *Community Standards*, FACEBOOK, https://www.facebook.com/communitystandards [https://perma.cc/2J3U-D4SA] ("Building community and bringing the world closer together depends on people's ability to share diverse views, experiences, ideas and information.").

[30] *The Twitter Rules*, TWITTER, https://help.twitter.com/en/rules-and-policies/twitter-rules [https://perma.cc/WZT9-4KKK] ("Our rules are to ensure all people can participate in the public conversation freely and safely.").

[31] *Community Guidelines*, GOOGLE, https://about.google/community-guidelines [https://perma.cc/SQK4-GY4D] ("Community guidelines exist to support the healthy and open discussion that has always been a part of our culture.").

[32] Minow, *supra* note 27, at 500 ("A majority of people in the United States now receive news selected for them by a computer-based mathematical formula derived from their past interests, producing echo chambers with few opportunities to learn, understand, or believe what others are hearing as news.").

[33] The marketplace-of-ideas model of the First Amendment finds its roots in Justice Oliver Wendell Holmes's "free trade in ideas" conception of free speech. *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting). According to this model, ideas must be allowed to compete freely in an unregulated market, whereby the best ideas will ultimately gain acceptance by competing with others in the marketplace. *See id.* Both Justice Holmes and Justice Louis Brandeis shared the belief that the proper remedy for harmful ideas in the marketplace is not censorship, but counterspeech. *See* Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring) ("[T]he remedy to be applied is more speech, not enforced silence."). The counterspeech doctrine posits "that 'bad speech' can be effectively countered or cured with more speech." Robert D. Richards & Clay Calvert, *Counterspeech 2000: A New Look at the Old Remedy for "Bad" Speech*, 2000 BYU L. REV. 553, 554.

[34] *See, e.g.*, Sarah Perez, *Plex Adds Personalized, Streaming News to Its Media Player Software*, TECHCRUNCH (Sept. 26, 2017, 8:00 AM), https://techcrunch.com/2017/09/26/plex-adds-personalized-streaming-news-to-its-media-player-software [https://perma.cc/UU7P-9M8Q] (describing Plex's new "personalized newscast that adapts to your interests based on what programming you watch and skip, among other things"); Casey Newton, *Google Introduces the Feed, a Personalized Stream of News on iOS and Android*, THE VERGE (July 19, 2017, 3:05 AM), https://www.theverge.com/2017/7/19/15994156/google-feed-personalized-news-stream-android-ios-app [https://perma.cc/R7TN-T8UJ] (discussing Google's new personalized news feed consisting "of articles, videos, and other content").

[35] Frank A. Pasquale, *The Automated Public Sphere*, *in* THE POLITICS OF BIG DATA: BIG DATA, BIG BROTHER? 110, 112 (Ann Rudinow Sætan, Ingrid Schneider & Nicols Green eds., 2018) ("Megafirms like Facebook and Google have largely automated the types of decisions once made by managers and programmers at television networks, or editors at newspapers.").

[36] Zeynep Tufekci, *Engineering the Public: Big Data, Surveillance and Computational Politics*, 19 FIRST MONDAY (2014), https://firstmonday.org/article/view/4901/4097 [https://perma.cc/2ZQL-RN8M] ("[Digital] platforms operate via algorithms the specifics of which are mostly opaque to people

The threat of political manipulation by rogue actors who deploy bots and use fake social media accounts has dominated the headlines.[37] Current scholarship has largely focused on the extent to which these illegitimate foreign and domestic operatives exploit the advertising tools of digital platforms to spread false and divisive messages;[38] however, more scholarly attention should be devoted to the ways in which these same technologies are exploited by legitimate political actors, such as politicians and campaigns, to win elections.

Recognizing the new possibilities offered by social media, political campaigns have increasingly turned to digital advertising to target voters.[39] By combining data-driven voter research with personalized advertising, political actors engage in political microtargeting, directing communications at niche audiences.[40] Online platforms provide a unique and powerful mechanism for influencing voters because they allow political ads to be targeted at certain audiences while remaining unseen by others, thus making it difficult for opposing candidates to counter targeted ads with their own messages.[41] During the 2016 election, the political-consulting company Cambridge Analytica reportedly exploited personal data from eighty-seven

outside the small cadre of technical professionals within the company with regards to content visibility, data sharing and many other features of political consequence.").

[37] *See, e.g.*, Adam Goldman, *Justice Dept. Accuses Russians of Interfering in Midterm Elections*, N.Y. TIMES (Oct. 19, 2018), https://www.nytimes.com/2018/10/19/us/politics/russia-interference-midterm-elections.html [https://perma.cc/6XW7-BEXW] (discussing federal charges against Russians alleged to have spread disinformation and attempted to interfere with the 2018 U.S. midterm elections).

[38] *See, e.g.*, Crain & Nadler, *supra* note 28, at 371 (assessing "policies for addressing the use of digital advertising systems by foreign operatives and other manipulative agents trying to influence elections, shape political discourse, inflame social division, and undermine democracy"); ELIZABETH BODINE-BARON, TODD C. HELMUS, ANDREW RADIN & ELINA TREYGER, COUNTERING RUSSIAN SOCIAL MEDIA INFLUENCE, at ix (2018) (analyzing "different approaches and policy options to respond to the specific threat of Russian influence on social media in the United States"). This Note uses the terms "legitimate" and "illegitimate" to distinguish between actors who are seeking office themselves versus political actors who seek to influence election results on behalf of other, hidden interest groups.

[39] *See, e.g.*, Jeff Chester & Kathryn C. Montgomery, *The Role of Digital Marketing in Political Campaigns*, 6 INTERNET POL'Y REV. 1, 2 (2017) ("[D]ata-driven digital marketing has moved into the centre of American political operations . . . .").

[40] Jacquelyn Burkell & Priscilla M. Regan, *Voting Public: Leveraging Personal Information to Construct Voter Preference*, *in* BIG DATA, POLITICAL CAMPAIGNING AND THE LAW: DEMOCRACY AND PRIVACY IN THE AGE OF MICRO-TARGETING 47, 60 (Normann Witzleb, Moira Paterson & Janice Richardson eds., 2020) (microtargeting is "achieved through the development of information-rich 'enhanced voter files' that integrate information from a wide range of sources[,] . . . . allow[ing] political communicators to reach particular voters with messages designed specifically to influence them").

[41] To increase advertising transparency, Facebook recently added an Ad Library feature that allows the public to access any active ads, including those hidden from users who were not part of an advertiser's intended audience. *See Ad Library*, FACEBOOK, https://www.facebook.com/ads/library [https://perma.cc/8S7N-V83L].

million Facebook users to sway voters to support Donald Trump's campaign.[42] Although Cambridge Analytica was shut down in 2018,[43] politicians and campaigns are increasingly reliant on similar data-collection and data-processing practices to target voters.[44] Most voters are unaware of how their personal data is continuously collected and weaponized by political actors.[45] The pervasive use of Big Data by political campaigns spotlights how digital platforms have enabled illegitimate and legitimate actors alike to manipulate voters, demonstrating the inextricable link between data-privacy protection and electoral integrity.

In response to the Cambridge Analytica scandal, Senator Dianne Feinstein introduced the Voter Privacy Act of 2019 on July 31, 2019, which was designed to provide voters with greater control over how their personal data is used in federal elections.[46] Two additional Democratic proposals, announced in May 2020, aimed at regulating how political campaigns can target ads.[47] These proposals remain stalled in Congress. Some social media companies have made preemptive changes. Google now limits its targeting parameters to age, gender, and general location,[48] and Twitter has banned

---

[42] *See* Cecilia Kang & Sheera Frenkel, *Facebook Says Cambridge Analytica Harvested Data of up to 87 Million Users*, N.Y. TIMES (Apr. 4, 2018), www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html [https://perma.cc/FC9J-7M4Y]; Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [https://perma.cc/QL7D-HLVA].

[43] *See* Colin Lecher, *Cambridge Analytica Is Shutting Down*, THE VERGE (May 2, 2018, 2:08 PM), https://www.theverge.com/2018/5/2/17311892/cambridge-analytica-us-offices-shutting-down-facebook-scandal [https://perma.cc/W89N-YY56].

[44] Gillian Tett, *Can You Win an Election Without Digital Skulduggery?*, FIN. TIMES (Jan. 9, 2020), https://www.ft.com/content/b655914a-3209-11ea-9703-eea0cae3f0de [https://perma.cc/VX8D-Y87X] (describing how Michael Bloomberg built a secretive data group called Hawkfish, which hired former Facebook employees and allegedly spoke to former Cambridge Analytica employees).

[45] *See Why Is Advertising Transparency Important?*, PRIV. INT'L (Aug. 5, 2019), https://privacyinternational.org/explainer/3288/why-advertising-transparency-important [https://perma.cc/RN3D-B6EA] ("At present, companies like Facebook, Google, and Twitter are not doing enough to provide their users with ads transparency. Importantly, in most countries around the world, users cannot understand why they're being targeted with political ads at all.").

[46] *See* Voter Privacy Act, S. 2398, 116th Cong. (2019). The bill would give voters five basic rights regarding their personal information: (1) right of access, (2) right of notice, (3) right of deletion, (4) right to prohibit transfer, and (5) right to prohibit targeting. *Id.*

[47] *See* Lauren Feiner, *Democratic Bills Aim at Cracking Down on Targeted Political Ads on Facebook and Google*, CNBC (May 26, 2020, 8:21 AM), https://www.cnbc.com/2020/05/26/democratic-bills-crack-down-on-political-ad-microtargeting-online.html [https://perma.cc/89G3-JRTJ].

[48] Rachel Sandler, *Google Limits Microtargeting for Paid Political Ads*, FORBES (Nov. 20, 2019, 8:22 PM), https://www.forbes.com/sites/rachelsandler/2019/11/20/google-limits-microtargeting-for-paid-political-ads/#63f3c93f51ec [https://perma.cc/SB7Q-FVNF].

political advertisements altogether.[49] Crucially missing from this list is Facebook, where as many as 43% of Americans consume their news,[50] and where as much as $797 million in political ads was projected to be spent during the 2020 election alone.[51] Despite mounting pressure, Facebook continued to allow microtargeting ahead of the 2020 election, and refused to police the truthfulness of its political ads.[52]

Outside of the political-advertising context, efforts to promote data privacy are unfolding at both the state and federal level.[53] Legislatures in twenty-five states and Puerto Rico either considered or enacted data-privacy bills in 2019.[54] An array of federal privacy bills have also been introduced in Congress.[55] In May of 2018, Vermont became the first state to regulate data

---

[49] Lauren Feiner, *Twitter Bans Political Ads After Facebook Refused to Do So*, CNBC (Oct. 30, 2019, 5:50 PM), https://www.cnbc.com/2019/10/30/twitter-bans-political-ads-after-facebook-refused-to-do-so.html [https://perma.cc/T3WA-X3FG].

[50] John Gramlich, *10 Facts About Americans and Facebook*, PEW RSCH. CTR. (May 16, 2019), https://www.pewresearch.org/fact-tank/2019/05/16/facts-about-americans-and-facebook [https://perma.cc/U7L7-VACW].

[51] Kate Gibson, *Spending on U.S. Digital Political Ads to Top $1 Billion for First Time*, CBS NEWS (Feb. 12, 2020, 6:10 PM), https://www.cbsnews.com/news/spending-on-us-digital-political-ads-to-cross-1-billion-for-first-time [https://perma.cc/LXH5-XSTB]. In the third quarter of 2020 alone, "political advertisers . . . spent at least $264 million on Facebook" ads. *See* Ari Levy, Salvador Rodriguez & Megan Graham, *Why Political Campaigns Are Flooding Facebook with Ad Dollars*, CNBC (Oct. 9, 2020, 12:32 PM), https://www.cnbc.com/2020/10/08/trump-biden-pacs-spend-big-on-facebook-as-election-nears.html [https://perma.cc/7MW4-B5MQ]. Facebook decided that it would stop featuring new political ads the week before the election as well as for a period of time following the election. *See* Mike Isaac, *Facebook Widens Ban on Political Ads as Alarm Rises over Election*, N.Y. TIMES (Nov. 17, 2020), https://www.nytimes.com/2020/10/07/technology/facebook-political-ads-ban.html [https://perma.cc/VA7G-6497].

[52] Associated Press, *Facebook Refuses to Restrict Untruthful Political Ads and Micro-Targeting*, GUARDIAN (Jan. 9, 2020, 9:13 AM), https://www.theguardian.com/technology/2020/jan/09/facebook-political-ads-micro-targeting-us-election [https://perma.cc/EH9P-GRGY]. Facebook started to label, but not fact-check, posts about the 2020 election by prompting users to visit USA.gov to receive official voting information. *See* Sonam Sheth, *Facebook Added a Label to Trump's Post Claiming That Voting by Mail Will Lead to a 'CORRUPT ELECTION,'* BUS. INSIDER (July 21, 2020, 9:59 AM), https://www.businessinsider.com/facebook-adds-label-trump-post-about-mail-in-voting-2020-7 [https://perma.cc/434W-29MA].

[53] Hamsini Sridharan & Margaret Sessa-Hawkins, *States Countering Digital Deception*, MAPLIGHT (June 25, 2019), https://maplight.org/story/states-countering-digital-deception [https://perma.cc/AYP4-D598].

[54] *2019 Consumer Data Privacy Legislation*, NAT'L CONF. OF STATE LEGISLATURES (Jan. 3, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy/calif.aspx [https://perma.cc/5S8K-Z82S].

[55] *See, e.g.*, Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019); Social Media Privacy Protection and Consumer Rights Act of 2019, S. 189, 116th Cong.; Online Privacy Act of 2019, H.R. 4978, 116th Cong.; American Data Dissemination Act of 2019, S. 142, 116th Cong.; Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019); Designing Accounting Safeguards to Help Broaden Oversight and

brokers.[56] California followed, enacting the nation's most comprehensive data-privacy law to date: the California Consumer Privacy Act (CCPA).[57] The CCPA requires companies to disclose to users what data is being collected about them and how it is used, and gives users the right to delete that data and prevent its sale.[58] Maine[59] and Nevada[60] came next, bringing the total to four enacted state laws. The Maine and Nevada bills differ in scope from the CCPA, previewing what is likely to become a complicated patchwork of laws with inconsistent or mutually exclusive requirements as more states enact their own privacy bills.[61] Compliance challenges for covered entities—especially tech companies—will only grow with the passage of each new state law, making a uniform federal bill imperative.[62]

Today's increasing calls for data-privacy regulation come as fundamental legal questions still remain unresolved: is personal data "speech" subject to First Amendment scrutiny, and, if so, what level of protection should it receive? Some scholars have argued that data-privacy

Regulations on Data, S. 1951, 116th Cong. (2019); Information Transparency and Personal Data Control Act, H.R. 2013, 116th Cong. (2019).

[56] *See* VT. STAT. ANN. tit. 9, § 2446 (2019); Devin Coldewey, *Vermont Passes First Law to Crack Down on Data Brokers*, TECHCRUNCH (May 27, 2018, 2:17 PM), https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers [https://perma.cc/YK62-CQJT]. Vermont's data-privacy law requires data brokers to register with the government, to report on whether they allow individuals to opt out of having their data collected or sold, and, if applicable, to specify the categories the opt-out does and does not apply to. tit. 9, § 2446.

[57] *See* Andy Green, *Complete Guide to Privacy Laws in the US*, VARONIS (Mar. 29, 2020), https://www.varonis.com/blog/us-privacy-laws [https://perma.cc/HKZ2-GCYN] ("[T]he CCPA is the most comprehensive internet-focused data privacy legislation in the US, and with no equivalent at the federal level.").

[58] *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100, .105, .120. The CCPA grants consumers a private right of action against businesses that fail "to implement and maintain reasonable security procedures and practices appropriate to the nature of the information." *Id.* § 1798.150.

[59] ME. STAT. tit. 35-A, § 9301 (2019). Maine's law imposes data-privacy requirements on internet service providers (ISPs), requiring them to obtain customer consent before they "use, disclose, sell or permit access" to consumer data. *See* An Act to Protect the Privacy of Online Customer Information, LD 946, 129th Leg. (Me. 2019). ISPs are required to take "reasonable measures" to protect customers' personal information from "unauthorized use, disclosure or access." *Id.*

[60] An Act Relating to Internet Privacy, SB 220, 80th Leg. (Nev. 2019). Nevada's law prohibits an operator of internet websites and online services from selling "personally identifiable information" to a third party without consent if a consumer has requested the data not be sold, but includes several exemptions. *See id.*

[61] Joseph J. Lazzarotti, Jason C. Gavejian & Maya Atrakchi, *Maine and Nevada Sign into Law Consumer Privacy Laws*, JACKSON LEWIS P.C. (July 3, 2019), https://www.workplaceprivacyreport.com/2019/07/articles/california-consumer-privacy-act/maine-and-nevada-sign-into-law-consumer-privacy-laws [https://perma.cc/JT8K-SXJL].

[62] *Id.*

restrictions constitute an impermissible form of speech regulation.[63] The Supreme Court's 2011 decision in *Sorrell v. IMS Health Inc.*[64] does not resolve this issue entirely but brings at least some data sharing within the protection of the First Amendment, potentially threatening online data-privacy regulations.[65] A First Amendment lawsuit has already unfolded over Maine's new data-privacy bill,[66] representing what is likely to be one of many legal challenges to the tide of recently enacted state laws.[67] Reconciling data privacy with the First Amendment is therefore a necessary precondition to the passage of a federal law.

Among the proposed state and federal privacy laws are the New York Privacy Act[68] and the Data Care Act.[69] These acts embody an emerging strain of thought in privacy circles first introduced in 2014 by Yale Law professor Jack Balkin,[70] which advocates for imposing fiduciary duties on online

---

[63] *See, e.g.*, Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 86 (2014) (arguing that data should be protected by the First Amendment); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1050–53 (2000) ("This article is an attempt to consider, as concretely as possible, the possible unintended consequences of various justifications for information privacy speech restrictions. I ultimately conclude that these consequences are sufficiently troubling that I must reluctantly oppose such information privacy rules.").

[64] 564 U.S. 552 (2011). In *Sorrell*, the Court held that a state statute restricting pharmaceutical marketers' access to and use of prescription data for advertising purposes violated the First Amendment as it constituted a content-based and speaker-based restriction on access to information and on speech employed for marketing purposes. *Id*. at 557, 563–64, 571.

[65] *See, e.g.*, Agatha M. Cole, *Internet Advertising After* Sorrell v. IMS Health*: A Discussion on Data Privacy & the First Amendment*, 30 CARDOZO ARTS & ENT. L.J. 283, 307 (2012) ("*Sorrell* does not provide a bright-line rule to assess the scope of First Amendment protection applicable to data. Rather, the opinion reveals a majority that is more likely to engage in a nuanced analysis that places more emphasis on context than medium.").

[66] *See* Jon Brodkin, *ISPs Sue Maine, Claim Web-Privacy Law Violates Their Free-Speech Rights*, ARS TECHNICA (Feb. 18, 2020, 1:43 PM), https://arstechnica.com/tech-policy/2020/02/isps-sue-maine-claim-web-privacy-law-violates-their-free-speech-rights [https://perma.cc/EEX5-3QPY]. On July 7, 2020, a federal judge rejected the ISPs' legal challenge, upholding Maine's data-privacy law. *See* Gabrielle Mannino, *Federal Judge Rules in Favor of Maine's Landmark Internet Privacy Law*, NEWS CTR. ME. (July 8, 2020, 11:09 AM), https://www.newscentermaine.com/article/news/local/federal-judge-rules-in-favor-of-maines-landmark-internet-privacy-law/97-0100d331-86ab-4bd6-ba9d-6af83f492db9 [https://perma.cc/PR5V-XGD6].

[67] *See* JENNIFER HUDDLESTON & IAN ADAMS, POTENTIAL CONSTITUTIONAL CONFLICTS IN STATE AND LOCAL DATA PRIVACY REGULATIONS 4 (2019), https://regproject.org/wp-content/uploads/RTP-Cyber-and-Privacy-Paper-Constitutional-Conflicts-in-Data-Privacy-final.pdf [https://perma.cc/X9UX-HFUV].

[68] *See* New York Privacy Act, S. 5642, 2019–2020 Leg., Reg. Sess. (N.Y. 2019).

[69] *See* Data Care Act of 2018, S. 3744, 115th Cong.

[70] *See* Jack M. Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (Mar. 5, 2014, 4:50 PM), https://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [https://perma.cc/VQU8-TZFF].

service providers[71] that collect and utilize personal data.[72] Ever since, Professor Balkin has been associated with the term "information fiduciary,"[73] which he defines as "a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship."[74] He argues that online service providers should be treated as information fiduciaries with respect to their end users, who entrust them with valuable personal information in exchange for their services.[75]

Treating online service providers as information fiduciaries would reconcile the First Amendment with data-privacy regulation. The First Amendment has not prevented the government from regulating how certain professionals, such as doctors and lawyers, use their clients' personal information, precisely because these professionals share a fiduciary relationship with their clients.[76] Therefore, consistent with the First Amendment, the government should be able to impose the same duties of care, loyalty, and confidentiality that define the traditional fiduciary relationship on online service providers.[77]

Professors Lina Khan and David Pozen have criticized Professor Balkin's proposal as an inadequate response to the structural power of online platforms, the problematic speech environment on social media, and the

---

[71] In this Note, "online service providers" refers to social media platforms, ISPs, email, news and entertainment providers, search engines, e-commerce, online banking or health sites, and other entities that collect personal data from end users in exchange for services.

[72] Press Release, Off. of Sen. Brian Schatz, Schatz Leads Group of 15 Senators in Introducing New Bill to Help Protect People's Personal Data Online (Dec. 12, 2018), https://www.schatz.senate.gov/press-releases/schatz-leads-group-of-15-senators-in-introducing-new-bill-to-help-protect-peoples-personal-data-online [https://perma.cc/B6E8-TB6A] ("By establishing a fiduciary duty for online providers, Americans can trust that their online data is protected and used in a responsible way."); Issie Lapowsky, *New York's Privacy Bill Is Even Bolder than California's*, WIRED (June 4, 2019, 7:00 AM), https://www.wired.com/story/new-york-privacy-act-bolder [https://perma.cc/7PK2-9C7A] (requiring New York businesses to act as "data fiduciaries," which "would legally bar businesses from using data in a way that benefits their companies to the detriment of their users").

[73] *See* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 499 (2019) ("Professor Kenneth Laudon appears to have coined this phrase [information fiduciaries] in the early 1990s. Since 2014, it has been identified with Professor Jack Balkin, who has developed the idea over a series of papers." (citation omitted)).

[74] *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1209 (2016).

[75] *Id.* at 1221–22.

[76] *Id.* at 1219 ("Information about clients that is obtained in the course of fiduciary relationships is not public discourse. Therefore, when a fiduciary communicates private information about a client to the public, the communication does not receive standard First Amendment protection, unless the dependent person—the client—permits the information to enter public discourse.").

[77] *See id.*

perverse economic incentives of targeted advertising.[78] Moreover, they challenge supporters of the information-fiduciary model to show what it adds to consumer-protection practices and why it should be viewed "as a promising path forward."[79]

This Note not only responds to Professors Khan and Pozen's criticisms, but also demonstrates how Professor Balkin's information-fiduciary approach can be applied to the issue of political microtargeting on digital platforms. Recognizing the limitations of Professor Balkin's proposal, this Note advocates for the passage of federal legislation that would instill online service providers with fiduciary duties towards their end users, superseding any duty owed to their shareholders. This Note then spells out how these fiduciary duties would be enforced, using political microtargeting on Facebook as an example, while also providing a model for their application in the broader context of targeted commercial advertising.

Part I lays out the main consequences associated with online political advertising, including voter manipulation, digital gerrymandering, and the exacerbation of social and political divisions. It then discusses why the traditional remedy for misleading or deceptive political ads—counterspeech—is no longer effective. Part II describes the shortcomings of the current notice-and-choice approach to regulating data privacy and how the First Amendment remains a barrier to meaningful reform. Part III demonstrates how Professor Balkin's information-fiduciary concept offers not only a viable approach for reconciling data privacy with the First Amendment, but also for responding to some of the most pressing challenges of our digital age. It begins with an overview of the fiduciary relationship, and then examines Professor Balkin's theory, as well as Professors Khan and Pozen's criticisms. Part III ends with a defense of the information-fiduciary approach to regulating data privacy. Part IV introduces a framework that applies Professor Balkin's information-fiduciary concept to the issue of political microtargeting on digital platforms. It then shows how this framework is applicable with equal force in the commercial-advertising context. This Note ends by discussing why the misinformation surrounding COVID-19 and the results of the 2020 presidential election makes the need for data-privacy reform more urgent than ever before.

---

[78] *See* Khan & Pozen, *supra* note 73, at 501–02, 540–41.

[79] *Id.* at 541.

I. THE DANGERS OF POLITICAL MICROTARGETING

The emergence of Big Data has revolutionized how political campaigns reach American voters. Through the combination of data-driven voter research and personalized advertising, political actors engage in political microtargeting on digital platforms.[80] Online platforms are a powerful instrument for influencing voters because they allow political ads to reach certain audiences while remaining unseen by others.[81] But most voters are unaware of how political actors exploit their personal data.[82] This is especially troubling given the "disturbing new opportunities for political manipulation and other forms of antidemocratic strategic communication" created by today's digital-advertising infrastructure.[83] Understanding the negative effects of political microtargeting on American democracy therefore proves vital to the development of an informed populace. This Part spotlights the main consequences associated with online political advertising, including voter manipulation, digital gerrymandering, and the exacerbation of social and political divisions. It then discusses why counterspeech—the traditional remedy for misleading or deceptive political ads—is no longer effective due to the opacity of political microtargeting.

A. Voter Manipulation

Although political campaigns have long used manipulative tactics to get their message out to voters, digital platforms have amplified the scope and power of these efforts, creating unprecedented opportunities for manipulation.[84] Today, campaigns weaponize digital-advertising technologies to target individuals who are most susceptible to strategic influence.[85] In essence, the personal data of American voters "is turned

---

[80] Burkell & Regan, *supra* note 40, at 47. A political advertiser could utilize Facebook's targeted advertising system to send a message only to Southern men without a college degree who earn less than $75,000. *See* Scott Rosenberg, *How Online Ad Targeting Weaponizes Political Misinformation*, AXIOS (Nov. 17, 2019), https://www.axios.com/online-ad-targeting-political-misinformation-3fac586c-2412-4c2b-a9c9-cbd2d47de6f8.html [https://perma.cc/49YE-G7RK].

[81] *See* ANTHONY NADLER, MATTHEW CRAIN & JOAN DONOVAN, WEAPONIZING THE DIGITAL INFLUENCE MACHINE: THE POLITICAL PERILS OF ONLINE AD TECH 1 (2018) ("[D]ata-driven advertising allows political actors to zero in on those believed to be the most receptive and pivotal audience for very specific messages while also helping to minimize the risk of political blowback by limiting their visibility to those who might react negatively.").

[82] *See* Burkell & Regan, *supra* note 40, at 63 ("The hyper-individualised nature of online communication . . . means that message manipulations are difficult to detect. As a result, voters may be unaware that they are being subjected to invisible persuasion by unidentified actors.").

[83] NADLER ET AL., *supra* note 81, at 4.

[84] *See* Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKELEY TECH. L.J. 449, 462 (2019).

[85] Crain & Nadler, *supra* note 28, at 372.

against them and used to help political advertisers more effectively influence their targets."[86] For instance, campaigns often resort to fear-mongering tactics, and "research shows that when afraid, only some people tend to become more conservative and vote for more conservative candidates."[87] But prior to digital advertising, campaigns had to target their fear-mongering messages to all voters (or at least a large subset), not just those likely to be receptive to such messages.[88] With the help of Big Data, campaigns can now target voters individually by using tactics designed to exploit their weaknesses and vulnerabilities.[89] Political microtargeting also allows messages to more easily escape the notice "of the press and the . . . public, markedly increasing their power to mislead and misinform viewers with impunity."[90] For example, a campaign can expose xenophobic voters to content about high crime rates among immigrants while evading political backlash from those more likely to respond negatively.[91]

Political microtargeting on digital platforms thus presents heightened opportunities for voter manipulation that directly threaten citizens' autonomy, undermining democracy in the process. "Personal autonomy is the capacity to make one's own choices, with respect to both existential and everyday decisions."[92] "[A]utonomy lies at the normative core of liberal democracies,"[93] as "democratic institutions are designed (ideally) to reflect autonomous decisions reached in the political sphere."[94] But when political campaigns target manipulative ads to those most vulnerable to influence, they attempt to circumvent voters' "capacity for reflection and

---

[86] *Id.*

[87] Tufekci, *supra* note 36.

[88] *Id.*

[89] *Id.*

[90] William A. Gorton, *Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy*, 38 NEW POL. SCI. 61, 72 (2016).

[91] *See* Frederik J. Zuiderveen Borgesius, Judith Möller, Sanne Kruikemeier, Ronan Ó Fathaigh, Kristina Irion, Tom Dobber, Balazs Bodo & Claes de Vreese, *Online Political Microtargeting: Promises and Threats for Democracy*, 14 UTRECHT L. REV. 82, 87 (2018). Facebook—the digital platform responsible for most political microtargeting, *see* Gibson, *supra* note 51—recently vowed to ban ads that claim "people from a specific race, ethnicity, national origin, religious affiliation, caste, sexual orientation, gender identity or immigration status are a threat to the physical safety, health or survival of others." Mark Zuckerberg, FACEBOOK (June 26, 2020), https://www.facebook.com/zuck/posts/10112048980882521 [https://perma.cc/X8TU-7UUD]. Facebook has not yet implemented this policy, and there is no indication of how rigorously it will be enforced or whether it will prove effective.

[92] Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 35 (2019).

[93] *Id.*

[94] *Id.* at 37.

deliberation."[95] Accordingly, political microtargeting has "clear implications for autonomy, which in turn has clear implications for democratic principles and practices."[96]

B. Digital Gerrymandering

The problem of digital gerrymandering can arise either from the algorithmic design of online platforms themselves or from the deliberate targeting decisions made by political advertisers. The term "digital gerrymandering" was first coined in 2014 by cyber-law scholar Jonathan Zittrain to describe how easily social media platforms like Facebook could exploit Big Data analytics to manipulate voter behavior and turnout.[97] In his provocative piece *Engineering an Election*, Professor Zittrain warns of the potential for digital platforms to engage in digital gerrymandering,[98] which he defines as "the selective presentation of information by an intermediary to meet its agenda rather than to serve its users."[99] He asks us to imagine a "hotly contested future election" where Facebook decides to gerrymander its users by selectively sending get-out-the-vote messages to only those supportive of a certain political candidate.[100] But Professor Zittrain's hypothetical threat is now a reality, as revealed by a recent study (Ali study) examining the impact of Facebook's ad-delivery algorithms on political ads.[101]

In the Ali study, a team of researchers ran a series of political ads on Facebook and tracked how they were delivered to different groups depending on the ad's content and targeting criteria. They found that Facebook's algorithms differentiate the price of reaching a user based on the user's

---

[95] CASS R. SUNSTEIN, THE ETHICS OF INFLUENCE: GOVERNMENT IN THE AGE OF BEHAVIORAL SCIENCE 82 (2016) (emphasis removed).

[96] Burkell & Regan, *supra* note 40, at 63.

[97] Jonathan Zittrain, Response, *Engineering an Election*, 127 HARV. L. REV. F. 335, 335–36 (2014). On November 2, 2010, Facebook subjected over sixty million American users to an experiment to see whether it could get them to vote in the U.S. congressional midterm elections when they otherwise would not have gone to the polls. *Id.* at 335. The results of the experiment revealed that users who received get-out-the-vote messages were 0.39% more likely to vote than users who did not receive them. *Id.* at 336. Researchers concluded this increased turnout directly by 60,000 voters and created a ripple effect that caused an additional 340,000 votes to be cast that day. *Id.*

[98] "Digital gerrymandering" has a broader meaning than "traditional gerrymandering," which more commonly refers to the manipulation of district boundaries to achieve an unfair political advantage for a certain party.

[99] Zittrain, *supra* note 97, at 336.

[100] *Id.*

[101] Muhammad Ali, Piotr Sapiezynski, Aleksandra Korolova, Alan Mislove & Aaron Rieke, *Ad Delivery Algorithms: The Hidden Arbiters of Political Messaging*, ARXIV (Dec. 17, 2019), https://arxiv.org/pdf/1912.04255.pdf [https://perma.cc/CU2A-E3HG].

inferred political alignment, which made it difficult for campaigns to reach voters across the political spectrum.[102] The study showed Facebook preferentially delivers ads to the users that it deems most "relevant," making it "cheaper and more effective for a political campaign to reach audiences that are politically aligned (as inferred by Facebook) with their agenda."[103] In essence, Facebook's algorithms make it more expensive for campaigns to get their message in front of users who do not already agree with them because Facebook yields a greater profit the longer users engage with content, revealing the extent to which polarization is an inextricable part of Facebook's business model.[104] This finding not only shows that Facebook's algorithms amplify social and political divisions—as explored in the next Section—but also demonstrates how Facebook's ad-delivery system engages in digital gerrymandering by pushing ads towards those already interested in the ad's content to "meet its agenda" of boosting profits "rather than to serve its users."[105]

A second type of digital gerrymandering can result from the deliberate choices made by political advertisers when sending out targeted ads. Researchers have shown that advertisers may exploit the advanced targeting features on Facebook to intentionally target or exclude users belonging to certain sensitive groups—a problem that still exists despite Facebook's decision to omit attributes such as "ethnic affinity" when sending ads related to housing, employment, or financial services.[106] In 2016, the Trump campaign was accused of using Facebook's targeting features to suppress Black votes by delivering negative Hillary Clinton ads to millions of African-American voters.[107] Moreover, the ability of political advertisers to

---

[102] *Id.* The researchers found that "Facebook delivers our ads with content from Democratic campaigns to over 65% users registered as Democrats, while delivering ads from Republican campaigns to under 40% users registered as Democrats, despite identical targeting parameters." *Id.*

[103] *Id.* The study found that it cost more to reach users across the political divide, costing 50% more to get a conservative voter to see Bernie Sanders content than Donald Trump content. *Id.*

[104] Gilad Edelman, *How Facebook's Political Ad System Is Designed to Polarize*, WIRED (Dec. 13, 2019, 7:00 AM), https://www.wired.com/story/facebook-political-ad-system-designed-polarize/ [https://perma.cc/258P-VSVM].

[105] Zittrain, *supra* note 97, at 336.

[106] *See* Till Speicher, Muhammad Ali, Giridhari Venkatadri, Filipe Nunes Ribeiro, George Arvanitakis, Fabrício Benevenuto, Krishna P. Gummadi, Patrick Loiseau & Alan Mislove, *Potential for Discrimination in Online Targeted Advertising*, 81 PROC. MACH. LEARNING RSCH. 1, 2, 14 (2018) (finding that despite banning the use of sensitive attributes such as ethnic affinity, "a malicious advertiser" can still "leverage the different targeting methods offered by platforms like Facebook to target users in a discriminatory manner").

[107] Philip Bump, *What We Know About Alleged Efforts by Trump's 2016 Campaign to Suppress Black Votes*, WASH. POST (Sept. 29, 2020, 3:36 PM), https://www.washingtonpost.com/politics/2020/09/29/what-we-know-about-efforts-by-trumps-2016-campaign-suppress-black-votes [https://perma.cc/

exclude unlikely voters from their advertising altogether "means that a strategy of focusing Presidential politics on 'swing states' can be implemented at an individual level."[108] In other words, "[a] home judged as a 'non–voter' can be skipped while the next one will be flooded with campaign material, thus introducing a new form of categorical inequality into the public sphere."[109]

In sum, digital gerrymandering can lead to voter suppression as well as to political campaigns ignoring entire subsets of the population deemed irrelevant to either the bottom line of the social media platform or the electoral chances of the political candidate. As a result, certain voters are discouraged to vote or purposefully underinformed and underrepresented in our democratic process.[110]

C. Social and Political Divisions

Political microtargeting also exacerbates social and political divisions. Social media ad systems "incentivize campaigns to not only target their messages, but to target them in ways that would further inflame and polarize opinions." [111] The Ali study shows how Facebook charges political advertisers a premium to reach audiences who are not already politically aligned with their party, disincentivizing campaigns to reach across party lines.[112] The algorithms of digital platforms such as Facebook are therefore designed to reinforce, rather than challenge, preexisting beliefs and stereotypes, deepening social and political divisions in our country.[113]

Furthermore, the opacity of political microtargeting has given rise to "a new type of 'dog whistle' politics, whereby a campaign emphasizes a provocative position only to sympathetic audiences, while remaining invisible to others."[114] This has made the prevalence of wedge issues all the

56Q3-FULT]. For instance, to discourage African Americans from voting, the Trump campaign directed the animation "Hillary Thinks African Americans Are Super Predators" to certain African-American voters on Facebook. *Id.*

[108] Tufekci, *supra* note 36.

[109] *Id*.

[110] Borgesius et al., *supra* note 91, at 87–88.

[111] *See* Casey Newton, *How Facebook Rewards Polarizing Political Ads*, THE VERGE (Oct. 11, 2017, 12:38 PM), https://www.theverge.com/2017/10/11/16449976/facebook-political-ads-trump-russia-election-news-feed [https://perma.cc/AJ33-22RE].

[112] Ali et al., *supra* note 101; *see also* Edelman, *supra* note 104.

[113] Minow, *supra* note 27, at 536 ("Amplifying prior views and predicted interests, the communication within social networks facilitated by digital companies may contribute to social division and polarization, even before enemies of the United States exploit them.").

[114] Tufekci, *supra* note 36.

more damaging as it enables campaigns to ignore "important but broadly relevant topics" such as the economy and education, and focus instead "on issues that can mobilize small, but crucial, segments."[115] For instance, a campaign wanting "to inflame feelings among rural and exurban communities that they are being looked down upon by urban elites" is now able to do so with increasing ease.[116] COVID-19 quickly developed into a major wedge issue for Democrats and Republicans who flooded social media with diametrically opposed ads about the nation's response to the pandemic, producing only "communicative confusion" over the severity of the virus itself.[117] Ultimately, digital political advertising, whether due to the algorithmic design of digital platforms or the deliberate efforts of political actors to exploit wedge issues, continues to inflame social and political divisions, weakening the stability of our democracy.

D. The Limited Efficacy of Counterspeech

The myriad harms associated with today's digital-advertising infrastructure highlight the extent to which counterspeech—the traditional remedy for false or deceptive speech in politics[118]—no longer serves as an adequate remedy in our increasingly fragmented and data-driven media environment.[119] A core "tenet of the First Amendment is that more speech is an effective remedy against the dissemination and consumption of false speech."[120] One of the assumptions underlying the counterspeech doctrine is that a significant portion of people exposed to false or misleading information will also be exposed to true or reliable information.[121] But the design of digital platforms prevents this type of exposure to counterspeech.[122] Through political microtargeting, political actors can send targeted messages

---

[115] *Id.*

[116] Crain & Nadler, *supra* note 28, at 379–80.

[117] Harry Dodsworth, *Federalism and Communicative Confusion in the Time of COVID-19*, NW. U. L. REV. NOTE (June 4, 2020), https://blog.northwesternlaw.review/?p=1453 [https://perma.cc/4YVZ-CKCL]; Yelena Mejova & Kyriaki Kalimeri, *COVID-19 on Facebook Ads: Competing Agendas Around a Public Health Crisis*, COMPASS '20: PROCS. 3D ACM SIGCAS CONF. COMPUTING & SUSTAINABLE SOC'YS 22, 29–30 (2020).

[118] *See* sources cited *supra* note 33 and accompanying text.

[119] *See* Dawn Carla Nunziato, *The Marketplace of Ideas Online*, 94 NOTRE DAME L. REV. 1519, 1521 (2019) ("[T]oday's online marketplace of ideas is besieged by the increased polarization and siloing of thought and opinion, which renders Holmes's prescribed remedy for harmful speech—counterspeech—increasingly ineffective.").

[120] Philip M. Napoli, *What If More Speech Is No Longer the Solution? First Amendment Theory Meets Fake News and the Filter Bubble*, 70 FED. COMMC'NS L.J. 55, 58 (2018).

[121] *Id.* at 61.

[122] *Id.* at 77.

to the most influenceable voters while hiding those messages from individuals likely to respond negatively.[123] The opaque nature of online political advertising is only exacerbated by digital platforms' algorithms, which push ads toward users already interested in their content, reducing exposure to political ads from across the aisle.[124] The limited efficacy of counterspeech within the context of political microtargeting demonstrates the importance of regulating data privacy to adequately respond to the harms associated with digital political advertising.

II. REGULATING DATA PRIVACY: THE CURRENT NOTICE-AND-CHOICE REGIME

Despite the importance of regulating data privacy, especially in the context of digital political advertising, the First Amendment remains a major barrier to reform. Many scholars maintain that any attempt to regulate the flow of personal data impermissibly restricts speech.[125] Leading "the 'First Amendment critique' of data privacy" is Professor Eugene Volokh.[126] According to Professor Volokh, "[T]he right to information privacy—my right to control your communication of personally identifiable information about me—is a right to have the government stop you from speaking about me."[127] He contends that any governmental regulation that restricts speakers' ability to communicate truthful data about other people is inconsistent with the First Amendment.[128] Professor Volokh concludes that "restrictions on

---

[123] *See supra* Section I.A.

[124] *See* Napoli, *supra* note 120, at 79 (explaining how the assumptions that underlie "[t]raditional approaches to counterspeech . . . . [are] at best quaint, and at worst utterly anachronistic, when applied to today's media environment of intertwined individual and algorithmic content filtering, in which filter bubbles have been constructed in ways that often are fundamentally oriented toward deflecting counterspeech").

[125] *See, e.g.*, FRED H. CATE, PRIVACY IN THE INFORMATION AGE 71 (1997) ("Any government effort to protect privacy . . . faces significant First Amendment obstacles."); SOLVEIG SINGLETON, CATO INST. POL'Y ANALYSIS, PRIVACY AS CENSORSHIP: A SKEPTICAL VIEW OF PROPOSALS TO REGULATE PRIVACY IN THE PRIVACY SECTOR 3 (1998) ("Regulations intended to protect privacy by outlawing or restricting the transfer of consumer information would violate rights of free speech.").

[126] Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1151 (2005) (defining "the 'First Amendment critique' of data privacy" as the belief that "any right of 'data privacy' is in direct conflict with the First Amendment because any attempt to regulate the flow of personal data would inevitably require the government to impose unconstitutional restrictions on speech").

[127] Volokh, *supra* note 63, at 1050–51.

[128] *See id.* at 1051. For a more recent First Amendment critique of data-privacy laws, see Bambauer, *supra* note 63, at 60–61, which argues that "freedom of speech carries an implicit right to create knowledge" and that when "the state regulates information precisely *because* it informs people, the regulation rouses the First Amendment."

speech that reveals personal information are constitutional under current doctrine only if they are imposed by contract, express or implied."[129] This contract-based approach to data privacy echoes what has now become a "hallmark of modern American privacy law[:] its reliance on a control-based regime of 'notice and choice.'"[130]

A. Notice and Choice

Underlying the current notice-and-choice regime of privacy law is the assumption that individuals can sufficiently handle and protect their own personal data through "privacy self-management."[131] The central components of privacy self-management are, first, notifying "individuals about the data collected and used about them (notice)" and then allowing individuals to choose whether or not to acquiesce to such collection and use (choice).[132] Privacy self-management originated in the Fair Information Practices (FIPs) developed in response to the rise of electronic databases.[133] "The FIPs represent a common understanding of the principles that organizations should follow to provide individuals with appropriate controls over the collection, use, and disclosure of their personal data, safeguard this data against security threats, and establish accountability measures that give effect to these principles."[134]

Privacy notices and the choice to opt out of certain types of data collection and uses are common features of modern privacy regulation.[135] The Federal Trade Commission (FTC) has enforced privacy notice

---

[129] Volokh, *supra* note 63, at 1122.

[130] Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 434 (2016).

[131] *Id.* at 444; *see also* Daniel J. Solove, *Introduction: Privacy Self-management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013) ("Under the current approach, the law provides people with a set of rights to enable them to make decisions about how to manage their data. These rights consist primarily of rights to notice, access, and consent regarding the collection, use, and disclosure of personal data.").

[132] Solove, *supra* note 131, at 1883.

[133] The FIPs were derived from a 1973 privacy report by the U.S. Department of Health, Education, and Welfare (HEW) in response to the growing use of automated data systems by public and private sector organizations. The report identified a "Code of Fair Information Practice" consisting of five core principles designed to protect the personal data these organizations were collecting. *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, DHEW PUB. NO. (OS) 73-94, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, at vi, xix–xxiii (1973).

[134] Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, 2014 WIS. L. REV. 861, 869.

[135] *See* Solove, *supra* note 131, at 1883–84.

requirements since the late 1990s,[136] finding breaches of such requirements to constitute "unfair or deceptive acts or practices in or affecting commerce" in violation of the Federal Trade Commission Act.[137] For instance, if the FTC detects a privacy violation, it can bring civil actions and seek injunctive remedies against the company at fault.[138] However, so long as companies notify consumers about their data collection, use, and disclosure practices in their privacy policies and give individuals the choice to opt out, they are free to exploit end-user data however they please.[139]

To scholars like Professor Volokh, privacy self-management is consistent with the First Amendment insofar as contract law protects users from companies that betray their own privacy policies with respect to their collection, use, and sale of personal data.[140] While Professor Volokh views privacy protection secured by contract to be constitutionally sound, he argues that "broader information privacy rules are not easily defensible under existing free speech law."[141]

However, many privacy scholars warn that relying solely on a notice-and-choice approach to privacy protection seriously underprotects people's privacy. [142] In the words of former FTC Chairman Jon Leibowitz, "[C]onsumers don't notice, read, or understand . . . privacy policies."[143] A

---

[136] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585 (2014).

[137] 15 U.S.C. § 45(a)(1).

[138] *See id.* § 45(l)–(m). In June 2016, the FTC fined the advertising company InMobi $950,000 for violating its own privacy policy. *See* Press Release, FTC, Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission (June 22, 2016), https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked [https://perma.cc/ACY5-P432].

[139] Richards & Hartzog, *supra* note 130, at 444 ("The most salient example of th[e] notice and choice regime is the ubiquitous privacy policy, that dense, unreadable, boilerplate text tucked away in some corner of virtually every website and application on the Internet.").

[140] *See* Volokh, *supra* note 63, at 1061 (finding no First Amendment problems with the government "simply enforcing obligations that the would-be speaker has himself assumed").

[141] *Id.* at 1051.

[142] *See, e.g.*, Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 341, 360–61 (Jane K. Winn ed., 2006) (explaining that privacy policies are long, difficult to understand, and rarely read); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1426–27 (2001) ("People must relinquish personal data to gain employment, procure insurance, obtain a credit card, or otherwise participate like a normal citizen in today's economy. Consent is virtually meaningless in many contexts. When people give consent, they must often consent to a total surrender of control over their information.").

[143] Jon Leibowitz, Comm'r, FTC, Remarks at the FTC Town Hall Meeting on "Ehavioral Advertising: Tracking, Targeting & Technology": So Private, So Public: Individuals, the Internet & the

study conducted by researchers at Carnegie Mellon revealed that it would take an average internet user seventy-six work days to review every privacy policy encountered over a year.[144] And even if consumers were to read the privacy policies they encounter on a daily basis, individuals often fail to conceptualize the value of their data and the consequences of giving it up.[145] Another study led by privacy journalist Julia Angwin found that choosing to opt out of data collection is practically akin to opting out of modern society, given the ubiquity of data surveillance in everyday life.[146]

Acclaimed privacy scholar Daniel Solove cogently summarizes the major problems plaguing privacy self-management as follows:

> (1) people do not read privacy policies; (2) if people read them, they do not understand them; (3) if people read and understand them, they often lack enough background knowledge to make an informed choice; and (4) if people read them, understand them, and can make an informed choice, their choice might be skewed by various decisionmaking difficulties.[147]

Accordingly, any "assumption that users have actual notice or meaningful choice is an illusion."[148]

B. The First Amendment Barrier

The inherent shortcomings of notice and choice highlight the inadequacy of privacy self-management and fuel demands for reform. However, the Supreme Court has so far embraced a more limited understanding of data privacy. In *Sorrell v. IMS Health Inc.*, one of its most recent rulings on data privacy, the Court struck down regulations limiting the communication and distribution of personal data about doctors.[149] Justice

---

Paradox of Behavioral Marketing 4 (Nov. 1, 2007), https://www.ftc.gov/sites/default/files/documents/public_statements/so-private-so-public-individuals-internet-paradox-behavioral-marketing/071031ehavior_0.pdf [https://perma.cc/E65D-5RS8].

144 Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, ATLANTIC (Mar. 1, 2012), http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-youencounter-in-a-year-would-take-76-work-days/253851 [https://perma.cc/X3YU-Y34N]; *see also* George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 J. INTERACTIVE MKTG. 15, 20 (2004) (finding only 4.5% of respondents always read website privacy notices and 14.1% frequently read them).

145 M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1149 (2011) ("Many consumers have little idea how much of their information they are giving up or how it will be used.").

146 *See* JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 153–67 (2014); *see also* Richards & Hartzog, *supra* note 130, at 444–45 (describing Julia Angwin as a leading privacy journalist).

147 Solove, *supra* note 131, at 1888.

148 Richards & Hartzog, *supra* note 130, at 444.

149 564 U.S. 552, 557 (2011).

Anthony Kennedy held the regulations unconstitutional because they served as content- and speaker-based restrictions on access to information and on speech utilized for marketing purposes.[150] While Justice Kennedy ultimately found it unnecessary to decide the question of whether data is protected speech under the First Amendment, his dicta characterizing the creation and dissemination of prescriber-identifying information as speech may be indicative of the Court's more narrow conception of data privacy.[151]

Especially in light of *Sorrell*, the First Amendment serves as a significant roadblock to the passage of any comprehensive federal privacy bill. A lawsuit already played out over Maine's new data-privacy law,[152] which prohibits certain internet companies from selling personal information, such as a customer's web-browsing history, geolocation data, and financial and health data, without the express consent of the customer.[153] While ultimately unsuccessful, the Maine lawsuit nevertheless represents what is likely to become one of many legal challenges to the recent wave of state data-privacy bills, demonstrating the importance of reconciling data privacy with the First Amendment.[154]

III. INFORMATION FIDUCIARIES AS THE VIABLE PATH FORWARD

Professor Balkin's information-fiduciary theory offers an effective framework for reconciling data privacy with the First Amendment. He contends that online service providers are information fiduciaries because users entrust them with sensitive information in exchange for their services.[155] As a result "of their special power over others and their special relationships to others," Professor Balkin argues that "information fiduciaries have special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute."[156] To understand Professor Balkin's information-fiduciary theory

---

[150] *See id.* at 563–64. Laws or regulations that are directed at certain content or aimed at particular speakers are presumptively invalid under the First Amendment and subject to heightened scrutiny. *Id.* at 567–71.

[151] *Id.* at 570–71 ("Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes.").

[152] *See* Brodkin, *supra* note 66.

[153] *See* An Act to Protect the Privacy of Online Customer Information, LD 946, 129th Leg. (Me. 2019).

[154] HUDDLESTON & ADAMS, *supra* note 67, at 12 ("In the absence of such a [federal] framework, not only will state laws fray the internet via a regulatory patchwork, but they will do so at the risk of creating tremendous legal uncertainty in the face of well-founded constitutional challenges.").

[155] *See* Balkin, *supra* note 74, at 1221.

[156] *Id.* at 1186.

and its implications for data-privacy regulation, it is important to first begin with an overview of the fiduciary relationship.

A. Defining the Fiduciary Relationship

"[A] fiduciary is an actor whom one should be able to trust to be loyal to one's interests."[157] While definitions vary, "[a] fiduciary relationship exists when one person places trust and confidence in another who, as a result, gains influence and superiority over the other."[158] "Fiduciary relationships stem from or create disparities of power and information, such that the relationship's beneficiary is or becomes vulnerable to the actor who occupies the fiduciary role."[159] Classic examples of fiduciary relationships include those between trustees and beneficiaries,[160] agents and principals,[161] lawyers and clients,[162] and doctors and patients.[163] Fiduciaries may manage property or money, or perform professional services for their beneficiaries, principals, or clients.[164] However, in nearly every instance, the fiduciary collects sensitive personal information that can be used to the beneficiary's disadvantage.[165] Because of the asymmetries of power and information that exist between the fiduciary and the beneficiary, "the main purpose of

---

[157] Deborah A. DeMott, *Relationships of Trust and Confidence in the Workplace*, 100 CORNELL L. REV. 1255, 1259 (2015); *see also* TAMAR FRANKEL, FIDUCIARY LAW 25 (2011) ("To perform their services, fiduciaries must be *entrusted* with various amounts of valuable assets and various degrees of discretion (power)." (emphasis added)).

[158] Kurtz v. Solomon, 656 N.E.2d 184, 190 (Ill. App. Ct. 1995); *see also* Calvin Klein Trademark Tr. v. Wachner, 123 F. Supp. 2d 731, 734 (S.D.N.Y. 2000) (noting that fiduciary relationships can arise "when one party's superior position or superior access to confidential information is so great as virtually to require the other party to repose trust and confidence in the first party").

[159] DeMott, *supra* note 157, at 1259 (citation omitted).

[160] *See* RESTATEMENT (THIRD) OF TRUSTS §§ 77–79 (AM. L. INST. 2007) (outlining the core fiduciary duties owed by trustees to their beneficiaries, including the duties of prudence, loyalty, and impartiality).

[161] *See* RESTATEMENT (THIRD) OF AGENCY § 8.01 (AM. L. INST. 2006) ("An agent has a fiduciary duty to act loyally for the principal's benefit in all matters connected with the agency relationship.").

[162] *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 7 cmt. b (AM. L. INST. 2000) ("The relationship between lawyer and client is one in which the lawyer generally owes the client rigorously enforced fiduciary duties, including duties of utmost good faith and fair dealing." (citation omitted)).

[163] *See e.g.*, S. SANDY SANBAR, ALLAN GIBOFSKY, MARVIN H. FIRESTONE & THEODORE R. LEBLANG, LEGAL MEDICINE 257 (4th ed. 1998) ("The relationship between patient and physician is one known to the law as a 'fiduciary relationship' . . . ."); Peter Bartlett, *Doctors as Fiduciaries: Equitable Regulation of the Doctor–Patient Relationship*, 5 MED. L. REV. 193, 199 (1997) ("[F]iduciary issues between doctors and patients are based in . . . the use or availability of information about the patient . . . .").

[164] Balkin, *supra* note 74, at 1207.

[165] *See id.* at 1207–08.

fiduciary law[] [is] to prohibit fiduciaries from misappropriating or misusing entrusted property or power."[166]

Traditional fiduciary relationships also give rise to the core duties of care, loyalty, and confidentiality. The duty of care is the duty to act competently and diligently by exercising an appropriate level of skill and prudence.[167] This is a *positive* duty that requires the fiduciary to use reasonable effort and diligence to promote the ends of the beneficiary.[168] The duty of loyalty is the duty to act in the beneficiary's best interest, rather than the fiduciary's own interest.[169] The duty of loyalty is a *negative* duty not to harm the beneficiary and to avoid conflicts of interest.[170] The duty of confidentiality is the duty to maintain the trust and confidence of the beneficiary and is intertwined with the duty of loyalty.[171] Under the duty of confidentiality, the fiduciary must exercise proper discretion and avoid wrongful disclosure of valuable or sensitive information collected from the beneficiary.[172] Finally, informed consent represents a critical aspect of the fiduciary relationship,[173] particularly in the medical profession.[174] To ensure

---

[166] FRANKEL, *supra* note 157, at 108.

[167] *In re* Schepps Food Stores, Inc., 160 B.R. 792, 797 (Bankr. S.D. Tex. 1993) ("The duty of care requires a director to exercise that degree of care that an ordinarily careful and prudent person would exercise under the same or similar circumstances.").

[168] *See* Arthur B. Laby, *Resolving Conflicts of Duty in Fiduciary Relationships*, 54 AM. U. L. REV. 75, 120 (2004) ("The fiduciary's duty of care . . . requires affirmative conduct to act in the principal's interest with respect to the assets or affairs of the principal entrusted to the fiduciary.").

[169] RESTATEMENT (THIRD) OF TRUSTS § 78 cmt. b (AM. L. INST. 2007) ("[A] trustee must refrain, whether in fiduciary or personal dealings with third parties, from transactions in which it is reasonably foreseeable that the trustee's future fiduciary conduct might be influenced by considerations other than the best interests of the beneficiaries.").

[170] Norlin Corp. v. Rooney, Pace Inc., 744 F.2d 255, 264 (2d Cir. 1984) ("[T]he duty of loyalty[] derives from the prohibition against self-dealing that inheres in the fiduciary relationship."); Laby, *supra* note 168, at 120 ("[T]he duty of loyalty . . . requires negative conduct . . . .").

[171] *See* RESTATEMENT (THIRD) OF TRUSTS § 78 cmt. i (AM. L. INST. 2007) ("Incident to the duty of loyalty . . . is the trustee's duty to preserve the confidentiality and privacy of trust information from disclosure to third persons . . . .").

[172] *See, e.g.*, Djowharzadeh v. City Nat'l Bank & Tr. Co., 646 P.2d 616, 619–20 (Okla. App. 1982) (finding a "[b]ank's relationship to a loan applicant implicitly imposes the duty to keep the contents of loan applications confidential"); Doe v. Roe, 400 N.Y.S.2d 668, 676, 679–80 (Sup. Ct. 1977) (finding a psychiatrist liable for breach of privacy, arising from the duty of confidentiality, for publication of a book containing disclosures about a patient during the course of psychotherapy).

[173] *See, e.g.*, Kalled v. Albee, 712 A.2d 616, 618 (N.H. 1998) ("Failure to obtain a client's informed consent constitutes a breach of fiduciary duty and a violation of public policy . . . ."); Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 483 (Cal. 1990) ("'[T]he patient's consent to treatment, to be effective, must be an informed consent,' . . . . [and] a physician has a fiduciary duty to disclose all information material to the patient's decision." (quoting Cobbs v. Grant, 502 P.2d 1, 9 (Cal. 1972))).

[174] The doctrine of informed consent requires that a physician disclose material facts relevant to the patient's decision about treatment. *See, e.g.*, Canterbury v. Spence, 464 F.2d 772, 780–83 (D.C. Cir. 1972)

that the beneficiary's interests are preserved, fiduciaries must obtain informed consent before engaging in actions that run counter to other core duties.[175]

Over time, fiduciary law has developed and expanded [176] to accommodate new relationships in areas such as family law, corporate law, agency law, banking law, employment law, and charities law.[177] Professor Balkin argues that today's digital economy calls for the recognition of a new type of fiduciary: online service providers.[178]

B. Balkin's Information-Fiduciary Theory

Professor Balkin finds that online service providers present many of the familiar problems that give rise to traditional fiduciary obligations.[179] First, much like an estate manager handles valuable assets, or a doctor manages sensitive patient records, online service providers collect personal information that is both highly valuable[180] and sensitive.[181] Second, like the disparities in power and expertise that exist between corporate directors and their shareholders, or lawyers and their clients, significant asymmetries of power and information are also apparent between online service providers

(describing how a "physician is under an obligation to communicate specific information to the patient when the exigencies of reasonable care call for it"); Thompson v. Gerowitz, 944 N.E.2d 1, 6 (Ind. Ct. App. 2011) ("Lack of informed consent is a distinct theory of liability premised on the physician's duty to disclose to the patient material facts relevant to the patient's decision about treatment.").

[175] *See, e.g.*, ANN. MODEL RULES OF PRO. CONDUCT § 1.7 (AM. BAR ASS'N 2019) (stating a lawyer must receive each affected client's informed consent to representation when a conflict of interest exists with a current client); RESTATEMENT (THIRD) OF AGENCY § 8.06 & cmt. a (AM. L. INST. 2006) (stating an agent must receive a principal's consent, among other requirements, to engage in conduct "that would otherwise constitute a breach of duty").

[176] *See* Tamar Frankel, *Fiduciary Law*, 71 CALIF. L. REV. 795, 796 (1983) ("The twentieth century is witnessing an unprecedented expansion and development of the fiduciary law.").

[177] *See* Tamar Frankel, *The Rise of Fiduciary Law* 9 (B.U. Sch. of L. Pub. L. Rsch. Paper No. 18-18, 2018), https://papers.ssrn.com/a=3237023 [https://perma.cc/D67Y-NG4K] ("Fiduciary relationships rise with (i) the dependence by people (entrustors) on the expertise of others (servicers) and (ii) the inability of the dependent persons to check the quality of the expertise and honesty of the servicers.").

[178] Balkin, *supra* note 74, at 1221–22.

[179] *Id.*

[180] *See, e.g.*, Richards & Hartzog, *supra* note 130, at 468 ("Personal information is valuable. In the technology industry, it is commonplace to state that 'data is the new oil,' meaning a fundamental source of value in the information economy."); Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 634 (2014) ("[O]nline firms' business models recognize the current and potential future value of consumers' personal information.").

[181] Sophisticated data-mining techniques are used to deduce extensive information about individuals who share even the most innocuous pieces of data. *See, e.g.*, Solove, *supra* note 131, at 1889–90 (discussing how innocuous pieces of data can "[u]nexpectedly . . . be combined and analyzed to reveal sensitive facts"). For instance, social media and online behavioral-tracking information can be used to predict personality traits as well as IQ and political affiliation. *See* Matz & Netzer, *supra* note 22, at 8.

and their end users.[182] Third, just as patients and clients depend on doctors and lawyers for the provision of critical medical or legal services, end users rely upon many of the services offered by digital platforms to participate and stay connected in the digital age.[183] Fourth, similar to doctors and lawyers who present themselves as reliable protectors of patient or client information, online service providers present themselves as trustworthy data collectors with benevolent motives, promising to deliver personalized content designed to optimize the user experience[184] and foster community and the spread of diverse voices and ideas online.[185]

In sum, just as fiduciary law imposes duties of care, loyalty, and confidentiality on estate managers, corporate directors, doctors, and lawyers, it follows that the law should also impose these special duties on digital platforms—like Facebook, Google, and Twitter—that exploit the personal data of their end users.[186] Such an approach allows for reconciling data privacy with the First Amendment.[187]

C. Information Fiduciaries and the First Amendment

Professor Balkin argues that there is an important distinction between speech that falls within public discourse, which receives standard First Amendment protection, and speech that falls outside of public discourse, which receives less protection.[188] This distinction depends not "on the content of the speech," but "on a characterization of social relationships."[189]

---

[182] *See* Jennifer Shkabatur, *The Global Commons of Data*, 22 STAN. TECH. L. REV. 354, 370 (2019) (describing concerns with "the immense information asymmetry between data platform companies and their users, and the obscure nature of the algorithms' operation"); Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 83 (2015) (stating that Big Data "introduces substantial new asymmetries of knowledge and power").

[183] *See* ANGWIN, *supra* note 146, at 153–67.

[184] *See* sources cited *supra* notes 1–7, 34 and accompanying text.

[185] *See* sources cited *supra* notes 29–31 and accompanying text.

[186] *See* Balkin, *supra* note 74, at 1226–27.

[187] The designation of online service providers as information fiduciaries is compatible with § 230 of the Communications and Decency Act, 47 U.S.C. § 230, which has long shielded online service providers from lawsuits based on content provided by third parties. *See* CONG. RSCH. SERV., REGULATING BIG TECH: LEGAL IMPLICATIONS 1 (Sept. 11, 2019), https://crsreports.congress.gov/product/pdf/LSB/LSB10309 [https://perma.cc/UM7C-43SQ]. But § 230 does not shield them from other forms of liability, such as privacy violations. *See* Natasha Singer & Mike Issac, *Facebook to Pay $550 Million to Settle Facial Recognition Suit*, N.Y. TIMES (Jan. 29, 2020), https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html [https://perma.cc/TW5U-6WUY].

[188] Balkin, *supra* note 74, at 1212–14. Professor Balkin defines public discourse as "the processes of communication through which ideas and opinions circulate in a community to produce public opinion." *Id.* at 1210.

[189] *Id.* at 1214.

When people participate in public discourse, "the law presumes that they are free, independent, and autonomous," and does not permit "restrictions on the dissemination of ideas and opinions."[190] But when people engage in speech outside of "public discourse, the law drops its assumption that everyone is equally able, independent, and knowledgeable."[191] Because "fiduciary law assume[s] that professionals and their clients do not stand on equal footing,"[192] it "does not treat speech in . . . fiduciary relationships as part of public discourse," but rather "as part of ordinary social and economic activity that is subject to reasonable regulation."[193] Professor Balkin provides the example of a lawyer or doctor who decides to run for office and who "reveals embarrassing information about clients to bolster his or her electoral chances," explaining: "Even though the content of the speech is political and its purpose is political, the speech is not immune from regulation, because it is an abuse of a confidential relationship in which the candidate was an information fiduciary."[194]

To further support his claim that the First Amendment treats speech in fiduciary relationships differently, Professor Balkin cites to four state court cases that recognize a doctor's duty not to disclose patient information.[195] He also points to the Supreme Court's decision in *Lowe v. SEC*[196] as signaling "that ordinary First Amendment doctrine—including even the ban on prior restraints—would not apply to communications between" certain professional fiduciaries and their beneficiaries.[197] Accordingly, he posits that treating online service providers as information fiduciaries provides a viable means for regulating their collection and use of personal data without violating the First Amendment.[198]

---

[190] *Id.* at 1214–15.

[191] *Id.* at 1215.

[192] *Id.* at 1216.

[193] *Id.* at 1217.

[194] *Id.* at 1219.

[195] *Id.* at 1210 n.120 (first citing Doe v. Roe, 400 N.Y.S.2d 668, 676 (Sup. Ct. 1977); then citing Horne v. Patton, 287 So. 2d 824, 829–30 (Ala. 1973); then citing Cannell v. Med. & Surgical Clinic, 315 N.E.2d 278, 280 (Ill. App. Ct. 1974); and then citing McCormick v. England, 494 S.E.2d 431, 439 (S.C. Ct. App. 1997)).

[196] 472 U.S. 181, 210–11 (1985) (upholding the right of people not registered as investment advisors to publish newsletters that offer advice about securities to the general public, but implying that Congress may treat investment advisors as fiduciaries if such communications developed "into the kind of fiduciary, person-to-person relationships . . . that are characteristic of investment adviser–client relationships").

[197] *See* Balkin, *supra* note 74, at 1219.

[198] *See id.* at 1225.

D. Criticisms of the Information-Fiduciary Approach

Professor Balkin's information-fiduciary theory has attracted praise from many scholars.[199] Lawmakers have also endorsed his approach, introducing legislation at both the federal[200] and state level[201] that incorporates his information-fiduciary concept. Despite garnering support in academic and political circles, Professor Balkin's model has been met with skepticism by Professors Lina Khan and David Pozen.

Professors Khan and Pozen have characterized his theory as an inapt response to the "business model . . . [and] outsized market share" of digital platforms.[202] One of their main criticisms is that several of the purported information fiduciaries, such as Facebook, Google, and Twitter, are Delaware corporations, and under Delaware corporate law, these companies "already owe fiduciary duties [] to the corporation and its stockholders."[203] Professors Khan and Pozen argue that today's leading social media "companies may be put in the untenable position of having to violate their fiduciary duties (to stockholders) under Delaware law in order to fulfill their fiduciary duties (to end users) under the new body of law that Balkin proposes."[204] The authors claim that digital companies like Facebook, Google, and Twitter would prove unable to manage the divided loyalties owed to their stockholders and end users, thus casting doubt on the practicability of the information-fiduciary model.[205]

---

[199] *See, e.g.*, ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 85 (2018) (endorsing the information-fiduciary model as an alternative to a "notice-and-choice" regime); Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. 1893, 1934 (2019) ("The information fiduciary frame provides perhaps the strongest possible footing for users to reassert control over how businesses use—and misuse—their information."); Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614, 625 (2018) ("[D]ata holders are properly understood as a subtype of what Jack Balkin calls 'information fiduciaries.'").

[200] Data Care Act, S. 3744, 115th Cong. (2018); *see also* Press Release, *supra* note 72 (describing the proposed legislation as "establishing a fiduciary duty for online providers").

[201] New York Privacy Act, S. 5642, 2019–2020 Leg., Reg. Sess. (N.Y. 2019); *see also* Lapowsky, *supra* note 72 (noting "the New York bill would . . . require businesses to act as . . . 'data fiduciaries'").

[202] Khan & Pozen, *supra* note 73, at 527–28. By "outsized market share," Professors Khan and Pozen refer to the market dominance of digital platforms such as Google and Facebook, which have together captured around "three-quarters of all digital advertising sales in the United States." *Id.* at 527. They argue "that any broad regulatory framework . . . for social media that focuses on abusive data practices, without attending to issues of market structure or political-economic influence," will prove ineffective. *Id*. at 528.

[203] *Id*. at 503.

[204] *Id*. at 504.

[205] *See id.* at 505–06. Reforms to make sites like Facebook "less addictive, to deemphasize sensationalistic material, and to enhance personal privacy would arguably be in the best interests of users.

Professors Khan and Pozen also contend that Professor Balkin "is all but silent on how these new duties would be enforced."[206] Moreover, they assert that his proposal "leave[s] many profound problems untouched."[207] They discuss how the speech environment on digital platforms has produced "a host of social ills, from facilitating interference in U.S. elections; . . . to enabling discrimination and harassment against women and racial minorities; to amplifying the influence of 'fake news,' conspiracy theories, bot-generated propaganda, and inflammatory and divisive content."[208] They argue that these broader harms are magnified "by a behavioral-advertising-based business model"[209] that incentivizes online platforms "to extract as much data from their users as they can—a motivation that runs headfirst into users' privacy interests."[210] They claim that Professor Balkin's proposal inadequately responds to the problems associated with the speech environment on digital platforms and with targeted-advertising-based business models.[211]

Finally, Professors Khan and Pozen suggest that his theory fails to account for how the Roberts Court would likely handle "First Amendment claims brought by online platforms" designated as information fiduciaries.[212] They point to the recent decision in *National Institute of Family & Life Advocates v. Becerra (NIFLA)*[213] as evidence of the Court's unwillingness to recognize professional speech as a separate category of protected speech,[214] undermining Professor Balkin's broader premise that the law treats speech in "professional or other fiduciary relationships . . . as part of ordinary social and economic activity that is subject to reasonable regulation."[215]

Yet each of these reforms would also pose a threat to Facebook's bottom line and therefore to the interests of shareholders." *Id.*

[206] *Id.* at 524.

[207] *Id.* at 526.

[208] *Id.* at 526–27 (citations omitted).

[209] *Id.* at 527.

[210] *Id.* at 512.

[211] *Id.* at 540–41.

[212] *Id.* at 531–32.

[213] 138 S. Ct. 2361 (2018). In *NIFLA*, the Court examined whether the disclosure requirements of a California reproductive-rights law violated the First Amendment. *Id.* at 2368. The law required that licensed clinics provide information to patients about free or low-cost services, such as abortions, and that unlicensed clinics notify patients of their unlicensed status. *Id.* The Court held that the disclosures violated the First Amendment, finding the licensed notice constituted an impermissible content-based regulation and the unlicensed notice unduly burdened protected speech. *Id.* at 2370–78.

[214] *Id.* at 2371–72 ("Speech is not unprotected merely because it is uttered by 'professionals.'").

[215] Khan & Pozen, *supra* note 73, at 531–32 (quoting Balkin, *supra* note 74, at 1217).

In sum, Professors Khan and Pozen identify several "ambiguities and tensions" in the information-fiduciary theory, as well as "concerns about the theory's capacity to resolve them satisfactorily."[216] The next Section responds to each of their criticisms in turn, making the case for why Professor Balkin's information-fiduciary approach should be viewed as a promising path forward.

E. A Defense of the Information-Fiduciary Approach

Although Professors Khan and Pozen raise legitimate concerns, their criticisms can be either refuted by case law or sufficiently addressed by clarifying how Professor Balkin's model might function in practice. Therefore, the goal of this Section is twofold: first, to respond to the criticisms that are already reconcilable, and second, to lay out the contours of an information-fiduciary approach that would adequately respond to their remaining concerns.

1. Reconcilable Criticisms

Although Professors Khan and Pozen rightly note that the Court has never explicitly recognized professional speech as its own special category, they fail to account for the extent to which professional speech—especially in the context of fiduciary relationships—is treated differently under the First Amendment than other types of speech.[217] Unlike most speech restrictions, laws addressing professional speech may in some instances be subject to only rational-basis review, making them more likely to pass muster under the First Amendment. Even Justice Clarence Thomas acknowledged this in his majority opinion in *NIFLA v. Becerra*,[218] noting that the Court has applied only rational-basis review to restrictions on professional speech in two circumstances: (1) where laws "require professionals to disclose factual, noncontroversial information in their 'commercial speech,'"[219] and (2) where

---

[216] *Id.* at 501.

[217] Claudia E. Haupt, *The Limits of Professional Speech*, 128 YALE L.J.F. 185, 188 (2018) ("[D]espite the Court's insistence that it has never recognized professional speech as a category, professional speech is distinct." (citation omitted)).

[218] 138 S. Ct. at 2372–73.

[219] *See id.* at 2372; *see also* Zauderer v. Off. of Disciplinary Couns. of Sup. Ct. of Ohio, 471 U.S. 626, 651 (1985) (upholding a rule requiring lawyers who advertised their services on a contingency-fee basis to disclose that clients will have to pay costs, finding that the disclosure requirement need only be "reasonably related to the State's interest in preventing deception of consumers"). The relaxed standard called for in *Zauderer* is viewed as akin to a rational-basis standard. *See, e.g.*, Nat'l Ass'n of Mfrs. v. SEC, 748 F.3d 359, 370–71 (D.C. Cir. 2014) ("The Supreme Court has stated that rational basis review applies to certain disclosures of 'purely factural and uncontroversial information.'" (quoting *Zauderer*, 471 U.S. at 651)); N.Y. State Rest. Ass'n v. N.Y.C. Bd. of Health, 556 F.3d 114, 132 (2d Cir. 2009) ("In

states regulate "professional conduct that incidentally burden[s] speech."[220] Rational-basis review, unlike intermediate or strict scrutiny, is a relaxed standard requiring that a law or regulation be only "rationally related" to a legitimate governmental interest to be constitutional.[221] Courts have afforded rational-basis review to restrictions on professional speech—especially that of doctors, lawyers, and other traditional fiduciaries—in four crucial realms[222]: professional licensing,[223] fiduciary duties,[224] informed consent,[225] and malpractice liability.[226] The fact that courts have carved out special exceptions for state regulation in these realms indicates that the First

light of *Zauderer*, this Circuit thus held that rules mandating that commercial actors disclose commercial information are subject to the rational basis test." (internal quotation marks omitted)).

[220] 138 S. Ct. at 2373; *see also* Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 457, 460–63 (1978) (upholding a disciplinary proceeding arising from a lawyer's in-person solicitation of clients where speech was "an essential but subordinate component" of the lawyer's conduct, finding that there was "a legitimate and important state interest" in regulation).

[221] *See* Micah L. Berman, *Clarifying Standards for Compelled Commercial Speech*, 50 WASH. U. J.L. & POL'Y 53, 59 (2016).

[222] *See* Haupt, *supra* note 217, at 190. Professional-licensing schemes represent "state laws enacted under the states' police powers" that are designed to ensure that patients and clients receive advice from qualified professionals. *Id.* Fiduciary duties and informed consent both "address the knowledge asymmetries between professionals and their clients or patients," with the former "creating duties of loyalty and care" that must be followed and the latter "ensuring that the interest in patient autonomy is protected. . . . Malpractice liability rests on the premise that . . . . [b]ad professional advice," as determined by the standards of the relevant knowledge community, "is subject to tort liability, and the First Amendment provides no defense." *Id.* at 191 (emphasis omitted).

[223] *See, e.g.*, Dent v. West Virginia, 129 U.S. 114, 128 (1889) (upholding a licensing requirement to practice medicine, concluding that "[t]he law of West Virginia was intended to secure such skill and learning in the profession of medicine that the community might trust with confidence those receiving a license under authority of the State"); Nat'l Ass'n for Advancement of Psychoanalysis v. Cal. Bd. of Psych., 228 F.3d 1043, 1056 (9th Cir. 2000) (upholding a licensing requirement for mental-health professionals against a First Amendment challenge).

[224] *See, e.g.*, Canterbury v. Spence, 464 F.2d 772, 781 (D.C. Cir. 1972) (outlining the duty of "due care" owed by a physician); Hendricks v. Clemson Univ., 578 S.E.2d 711, 716 (S.C. 2003) ("Historically, [the South Carolina Supreme Court] has reserved imposition of fiduciary duties to legal or business settings, often in which one person entrusts money to another, such as with lawyers, brokers, corporate directors, and corporate promoters.").

[225] *See, e.g.*, Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 884 (1992) (plurality opinion) (upholding a law requiring physicians to obtain informed consent before they could perform an abortion, finding that "the physician's First Amendment rights not to speak are implicated, but only as part of the practice of medicine, subject to reasonable licensing and regulation by the State" (citations omitted)); Cruzan v. Director, Mo. Dep't of Health, 497 U.S. 261, 269 (1990) ("The informed consent doctrine has become firmly entrenched in American tort law.").

[226] *See, e.g.*, NAACP v. Button, 371 U.S. 415, 438 (1963) (noting that while torts for legal malpractice "fall within the traditional purview of state regulation of professional conduct," the subject of professional standards does not outweigh First Amendment rights of NAACP lawyers); Shea v. Bd. of Med. Exam'rs, 146 Cal. Rptr. 653, 661 (Ct. App. 1978) (holding a doctor whose "conduct violated the trust reposed in him by his patients" liable for malpractice).

Amendment treats fiduciary relationships differently in practice. Professors Khan and Pozen's skepticism about First Amendment flexibility as applied to fiduciary relationships thus runs counter to "centuries of equity, torts, and other common law doctrine."[227]

Professors Khan and Pozen do raise the valid point that "[e]ven if the Court . . . [has] some sort of relaxed standard of First Amendment review for regulations of traditional fiduciary–beneficiary communications, it is not at all clear that the Court would apply this standard to the special case of digital information fiduciaries."[228] They argue that Professor "Balkin's crucial concession that the fiduciary duties owed by [digital] platforms" would be more limited than those owed by traditional fiduciaries means that state regulation would have to be more limited as well.[229] But these insights only reaffirm the importance of narrowly tailoring the duties owed by online service providers to what should reasonably be expected of them based on the services they offer.[230]

For instance, doctors are reasonably expected to warn patients about health risks precisely because doctors "present themselves as learned professionals concerned with our health."[231] Unlike doctors, digital platforms "do not hold themselves out as taking care of end-users in general" but as helping users "connect with other people," which they accomplish through their collection and use of end-user data.[232] Therefore, a company like Facebook would not be reasonably expected to warn users not to watch an emotionally disturbing video or befriend a dangerous person but would be expected to provide users with meaningful control over their personal data and warn them about the consequences of Facebook's data collection and use practices.[233]

There are important differences between traditional fiduciaries and digital-information fiduciaries, necessitating that we "connect the kinds of duties that information fiduciaries have to the services they provide."[234] But assuming a strong enough case is made for designating online service providers as information fiduciaries,[235] these differences should not affect the

---

[227] Richard S. Whitt, *Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era*, 36 SANTA CLARA HIGH TECH. L.J. 75, 86 (2019).

[228] Khan & Pozen, *supra* note 73, at 532.

[229] *Id.*

[230] *See* Balkin, *supra* note 74, at 1229.

[231] *Id.* at 1228.

[232] *Id.*

[233] *See id.* at 1228–29.

[234] *Id.* at 1229.

[235] *See supra* Section III.B.

Court's willingness to apply a relaxed First Amendment standard of review for regulations of digital platforms.[236]

Professors Khan and Pozen's remaining criticisms focus less on the constitutionality of the information-fiduciary model than on its actual effectiveness in remedying the problems associated with the speech environment on social media and with targeted-advertising business models.[237] The following Section lays out the contours of an information-fiduciary approach that would adequately respond to their remaining concerns.

2. A "Promising" Information-Fiduciary Model

Professors Khan and Pozen correctly point out that, in the absence of "heavy-handed government intervention,"[238] digital platforms would prove unable to manage their divided loyalties to their stockholders and end users.[239] But enactment of a federal statute would solve this problem by explicitly imposing on online service providers fiduciary duties toward their end users, superseding any duties owed to their shareholders. The proposed New York Privacy Act offers a useful model for managing the divided loyalties of digital platforms, stating that

> [e]very legal entity, or any affiliate of such entity, and every controller and data broker, which collects, sells or licenses personal information of consumers, shall exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and shall act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker, in a manner expected by a reasonable consumer under the circumstances.[240]

A federal statute "that clearly prioritizes"[241] the fiduciary duties owed by online service providers to their end users would preempt any existing obligations owed by Delaware corporations—such as Facebook, Google, and Twitter—to their stockholders under Delaware law.[242] Accordingly,

---

[236] *See* sources cited *supra* notes 217–227 and accompanying text.

[237] Khan & Pozen, *supra* note 73, at 540–41.

[238] *Id.* at 504 (quoting Jonathan Zittrain, *How to Exercise the Power You Didn't Ask For*, HARV. BUS. REV. (Sept. 19, 2018), https://hbr.org/2018/09/how-to-exercise-the-power-you-didnt-ask-for [https://perma.cc/EAN3-KCYC]).

[239] *Id.* at 508 ("Balkin has never squarely addressed the issue of crosscutting loyalties.").

[240] S. 5642, § 1102, 2019–2020 Leg., Reg. Sess. (N.Y. 2019).

[241] Khan & Pozen, *supra* note 73, at 504.

[242] *See* U.S. CONST. art. VI, cl. 2 ("This Constitution, and the Laws of the United States which shall be made in Pursuance thereof . . . shall be the supreme Law of the Land . . . ."); *see also* Gade v. Nat'l

Professors Khan and Pozen's concern about the "crosscutting loyalties" of online platforms[243] would no longer apply, as federal law would mandate that these entities put the interests of their end users first.

Passing any federal legislation in today's difficult political environment is challenging, at best, but there are several reasons to be hopeful about this particular proposal. As it currently stands, Professor Balkin's information-fiduciary approach already enjoys some bipartisan support.[244] Although congressional gridlock has so far hindered the passage of a federal data-privacy bill,[245] the 2020 election has resulted in a unified national government[246] that may prove capable of pushing through legislation. Furthermore, the model has gained praise from Mark Zuckerberg[247]—one of Big Tech's most powerful voices—signaling that the information-fiduciary approach may also have the backing of the tech industry. The current "patchwork of state and local laws about online privacy" has made a uniform federal bill increasingly desirable to tech companies wishing to escape the uncertainty of legal liability.[248] Since going into effect in January of 2020,

---

Solid Wastes Mgmt. Ass'n, 505 U.S. 88, 98 (1992) (outlining the doctrine of preemption, which holds that federal law supersedes conflicting state law).

[243] *See* Khan & Pozen, *supra* note 73, at 508. Professors Khan and Pozen raise the legitimate concern that reforms implicating the business models of online service providers, like Facebook, may pose a threat to their bottom line and to the interests of shareholders. *Id.* at 506. But as this Note later points out, the government has a legitimate interest in promoting electoral integrity, making any fiscal consequences born on online service providers sufficiently warranted. *See infra* Section IV.A.2.

[244] *See, e.g.*, 164 CONG. REC. S2026 (Apr. 10, 2018) (statement of Republican Sen. John Cornyn) ("Perhaps we should treat social media platforms as information fiduciaries and impose legal obligations on them, as we do with lawyers and doctors, who are privy to some of our most personal, private information."); Data Care Act of 2018, S. 3744, 115th Cong. (codifying legislation proposed by fifteen Democratic senators establishing fiduciary duties for online providers).

[245] *See, e.g.*, Müge Fazlioglu, *Tracking the Politics of US Privacy Legislation*, INT'L ASS'N PRIVACY PROS. (Dec. 13, 2019), https://iapp.org/news/a/tracking-the-politics-of-federal-us-privacy-legislation [https://perma.cc/H5Q2-R65V] ("[A]ny successful privacy legislation will require bipartisan support."); Charlie Warzel, *Will Congress Actually Pass a Privacy Bill?*, N.Y. TIMES (Dec. 10, 2019), https://www.nytimes.com/2019/12/10/opinion/congress-privacy-bill.html [https://perma.cc/36ZL-SUEJ] (discussing how disagreements between Democrats and Republicans have stalled the passage of a federal privacy bill).

[246] *See* Michael Scherer, *Democrats Win Unified — if Narrow — Control of Washington on a Violent Day*, WASH. POST (Jan. 6, 2021, 9:04 PM), https://www.washingtonpost.com/politics/senate-democrats-ossoff-warnock/2021/01/06/5c9ec09e-5031-11eb-83e3-322644d82356_story.html [https://perma.cc/GTD6-E8U6].

[247] *At Harvard Law, Zittrain and Zuckerberg Discuss Encryption, 'Information Fiduciaries' and Targeted Advertisements*, HARV. L. TODAY (Feb. 20, 2019), https://today.law.harvard.edu/at-harvard-law-zittrain-and-zuckerberg-discuss-encryption-information-fiduciaries-and-targeted-advertisements/ [https://perma.cc/K73X-PAT2] ("The idea of [Facebook] having a fiduciary relationship with the people who use our services is intuitive.").

[248] Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-

the CCPA—through its private cause of action—has already triggered at least forty-six lawsuits,[249] highlighting how compliance with stronger state laws has become especially burdensome for tech companies.[250] A federal statute that offers the imposition of fiduciary duties in exchange for federal immunity from conflicting state and local regulations would likely appeal to Big Tech,[251] making its enactment politically feasible.

Professors Khan and Pozen also characterize Professor Balkin's proposal as an inadequate response to the broader harms produced by social media—such as electoral interference, discrimination against women and minorities, and the spread of fake news[252]—and the problematic incentives of targeted advertising where companies are "economically motivated to extract as much data" as possible from their users.[253] However, applying the information-fiduciary model to the issue of political microtargeting on Facebook shows how Professor Balkin's approach could effectively respond to the issues plaguing the speech environment on social media as well as the problems inherent in targeted advertising more generally.

In Part IV, this Note argues that the information-fiduciary concept, when applied to Facebook, would require both (1) the expansion of Facebook's current notice-and-choice framework for receiving end-user consent to run microtargeted political ads, and (2) the imposition of a new liability regime that subjects Facebook to the fiduciary duties of care, loyalty, and confidentiality towards its end users' data. Holding Facebook and other digital platforms that engage in political advertising to an information-fiduciary standard would ameliorate some of the adverse effects of political microtargeting and address the broader societal goal of promoting electoral

---

fiduciary/502346 [https://perma.cc/NR4X-TD97]; *see also* Dina Temple-Raston, *Why the Tech Industry Wants Federal Control over Data Privacy Laws*, NAT'L PUB. RADIO (Oct. 8, 2018), https://www.npr.org/2018/10/08/654893289/why-the-tech-industry-wants-federal-control-over-data-privacy-laws [https://perma.cc/64Z5-FFVA] (stating that Big Tech companies want federal regulation "that would pre-empt state laws" to "avoid a patchwork of rules in different states"). For more on Big Tech's push for federal privacy legislation, see Sebastian Herrera, *Tech Giants' New Appeal to Governments: Please Regulate Us*, WALL ST. J. (Jan. 27, 2020, 7:01 AM), https://www.wsj.com/articles/tech-giants-new-appeal-to-governments-please-regulate-us-11580126502 [https://perma.cc/L6JC-DCNC], and Jeff Horwitz & Deepa Seetharaman, *Facebook's Zuckerberg Backs Privacy Legislation*, WALL ST. J. (June 26, 2019, 7:54 PM), https://www.wsj.com/articles/facebooks-zuckerberg-backs-privacy-legislation-11561589798 [https://perma.cc/9B7M-AL2D].

[249] Phil Yannella, Kim Phan & Greg Szewczyk, *An Early Look at California Consumer Privacy Act Litigation Trends*, LAW.COM (July 16, 2020, 2:26 PM), https://www.law.com/thelegalintelligencer/2020/07/16/an-early-look-at-california-consumer-privacy-act-litigation-trends [https://perma.cc/Z8HE-6XWV].

[250] Balkin & Zittrain, *supra* note 248.

[251] *See* sources cited *supra* note 248 and accompanying text.

[252] Khan & Pozen, *supra* note 73, at 526–27.

[253] *Id.* at 512.

integrity in our digital age. Most importantly, this proposed framework is not limited to political advertising but is equally applicable in the commercial-advertising context, offering a promising path forward for responding to some of the most pressing challenges of today's digital landscape.

IV. THE ADOPTION OF AN INFORMATION-FIDUCIARY STANDARD

This final Part offers a proposed framework for enforcing Professor Balkin's model on digital platforms that engage in political microtargeting by specifically examining what enforcement would look like on Facebook—the social media platform running the most political ads. It then demonstrates the broader applicability of this framework to the commercial advertising context.

A. An Information-Fiduciary Approach to Political Microtargeting

As stated, treating Facebook as an information fiduciary would require (1) the expansion of Facebook's current notice-and-choice framework for receiving end-user consent to run microtargeted political ads, and (2) the imposition of a liability regime that subjects Facebook to the fiduciary duties of care, loyalty, and confidentiality when handling end-user data.

1. Expansion of Facebook's Current Notice-and-Choice Framework

Under an information-fiduciary regime, Facebook would have to significantly revamp its approach to obtaining end-user consent to run microtargeted political ads. Much like other digital platforms, Facebook relies on a notice-and-choice regime for garnering consent to collect and use the personal data of its end users.[254] By providing individuals with *notice* about the data collected and used about them and giving individuals the *choice* to opt out of such collection and uses, Facebook operates under the assumption that its end users can sufficiently handle and protect their own personal data through privacy self-management. [255] However, this assumption is illusory,[256] especially in the context of political microtargeting.

For instance, on the "About Facebook Ads" page, Facebook informs individuals why advertisers may be showing users particular ads and gives them the choice to modify their ad preferences.[257] But crucially missing is

---

[254] *Data Policy*, FACEBOOK, https://www.facebook.com/policy.php [https://perma.cc/Y769-V7U6]. For further information about notice-and-choice consent regimes, see Richards & Hartzog, *supra* note 130, at 434, 444.

[255] *See* Richards & Hartzog, *supra* note 130, at 444.

[256] *Id.*

[257] *About Facebook Ads*, FACEBOOK, https://www.facebook.com/about/ads [https://perma.cc/VR9S-V8CC].

any discussion of the consequences of political microtargeting. Informed consent constitutes a fundamental aspect of the fiduciary relationship.[258] However, Facebook's failure to include warnings about the risks associated with political microtargeting renders any "consent" to run microtargeted ads effectively meaningless, spotlighting the need for Facebook to implement a new system for obtaining *informed* consent from its end users.

First, Facebook would have to provide its users with *adequate* notice. This requires more than just notifying users about how their personal data influences what ads they are shown, but actually informing users about the negative effects of political microtargeting. Disclosure in the Health Insurance Portability and Accountability Act (HIPAA) context offers a useful analogue for conceptualizing how to provide Facebook users adequate notice about political microtargeting. Before a patient can give informed consent for a medical operation, the service provider must disclose enough information so that the patient can make an informed decision.[259] While the patient need not receive every small detail about a medical procedure, the patient must, at a minimum, receive information in plain language about the potential risks or benefits associated with the procedure and any other information that would be expected by a reasonable person to make an informed decision.[260]

The same should hold true in the context of political microtargeting on Facebook. Just as medical patients cannot be expected to provide informed consent to an operation without receiving information about the risks and benefits of the procedure, Facebook users cannot be expected to provide informed consent to receive targeted ads without obtaining information about the risks and benefits of political microtargeting. For users to give informed consent to receive microtargeted political ads, Facebook must provide its users with enough information to make an informed decision. Details about how political advertising on Facebook can lead to voter manipulation, digital gerrymandering, and the exacerbation of political and social divisions is precisely the type of information that would be expected by a reasonable person to make an informed decision.[261] For instance, Facebook should warn users that when receiving political ads, they may be

---

[258] *See* sources cited *supra* notes 173–174, 225 and accompanying text.

[259] *See* sources cited *supra* notes 173–174, 225 and accompanying text.

[260] *See, e.g.*, Crain v. Allison, 443 A.2d 558, 562 (D.C. Cir. 1982) ("[A]t a minimum, a physician must disclose the nature of the condition, the nature of the proposed treatment, any alternate treatment procedures, and the nature and degree of risks and benefits inherent in undergoing and in abstaining from the proposed treatment.").

[261] *See supra* Part I.

uniquely susceptible to strategic influence or manipulation based on their data profile.[262] Facebook should inform users that because of digital gerrymandering, they may be targeted with certain ads aimed to suppress their vote or be purposefully excluded from advertising altogether.[263] Facebook should also notify users that they may only be seeing ads that reinforce their preexisting views or that are intentionally inflammatory.[264]

Users need not receive exhaustive detail about political microtargeting, but they should, at a minimum, receive a brief synopsis in plain language of the potential risks associated with this practice and links to additional resources—preferably official government websites—to learn more about political microtargeting. The information could be displayed in the form of a pop-up message each time a user receives a microtargeted political ad; however, Facebook could give users the option to deactivate the pop-up message from appearing on future political ads.

Courts would likely treat a mandated disclosure about political microtargeting as compelled commercial speech subject to *Zauderer*'s rational-basis test, requiring that it contain only "factual, noncontroversial information" and be "reasonably related" to a legitimate governmental interest.[265] Federal legislation compelling Facebook and other digital platforms to communicate the risks of political microtargeting would likely satisfy *Zauderer*, as disclosure of such information *reasonably relates* to the government's legitimate interest in promoting electoral integrity.[266]

Second, Facebook must provide its users with *meaningful* choice over how to receive political ads. For users to possess meaningful choice, they must have the opportunity to shape their political-advertising experiences in clear and tangible ways. The problem with Facebook's current approach is not that users lack actual choices—in fact, users possess quite a few ways to alter their ad preferences—but that users have no way of conceptualizing how their choices affect the types of ads they are shown.

On the "Ad Preferences" page, users can select whether to receive ads based on relationship status, employer, job title, education, and other categories set by Facebook, as well as whether to temporarily or permanently hide ad topics from appearing in their newsfeed.[267] Users can also opt out of

---

[262] *See supra* Section I.A.

[263] *See supra* Section I.B.

[264] *See supra* Section I.C.

[265] *See* sources cited *supra* notes 219, 221 and accompanying text.

[266] *See supra* note 219.

[267] *See What Are My Ad Preferences and How Can I Adjust Them on Facebook?*, FACEBOOK, https://www.facebook.com/help/247395082112892 [https://perma.cc/78FV-XVQ7].

receiving ads based on data collected from Facebook's partners or from Facebook Company Products,[268] such as Instagram and WhatsApp.[269] But Facebook does not give users a clear sense of how their newsfeeds would change with certain ad settings, leaving users with no way of knowing whether they should adjust their ad preferences.

Facebook's Ad Preferences page should be modified so that when users click on a specific setting, they are provided with examples of political ads in their newsfeed that appear because of that setting.[270] For instance, say a user is deciding whether to opt out of receiving ads based on her education, but would like to understand the types of ads that are influenced by this setting. By clicking on the education setting, the user should be able to see examples of political ads that she received because of her education, allowing her to make a more informed decision about whether to disable this setting. By providing users with a better sense of how their political ads are targeted, users will likely be more inclined to modify how they receive political ads, given that most Americans oppose microtargeting in the first place.[271]

2. Imposition of Fiduciary Duties of Care, Loyalty, and Confidentiality

As an information fiduciary, Facebook would also be expected to abide by the duties of care, loyalty, and confidentiality in its handling of end-user data. Essentially, Facebook would be required to honor and promote the choices of its end users regarding how their personal data can be used for political microtargeting purposes.

Under the duty of care, Facebook would be obligated to advance the interests of its end users. For users that either opt out of receiving microtargeted political ads entirely or modify how their data can be used,

---

[268] *See The Facebook Company Products*, FACEBOOK, https://www.facebook.com/help/195227921252400 [https://perma.cc/65HY-4K6A].

[269] *See How Can I Adjust How Ads on Facebook Are Shown to Me Based on Data About My Activity From Partners?*, FACEBOOK, https://www.facebook.com/help/568137493302217 [https://perma.cc/EM6D-XYQ5].

[270] Although users are able to click on an ad in their newsfeed to learn about why they are seeing it, *see How Does Facebook Decide Which Ads to Show Me?*, FACEBOOK, https://www.facebook.com/help/562973647153813 [https://perma.cc/DNW6-27JY], this requires users to engage in a piecemeal process of figuring out how their data is used by different political advertisers.

[271] Justin McCarthy, *In U.S., Most Oppose Micro-targeting in Online Political Ads*, GALLUP (Mar. 2, 2020), https://news.gallup.com/opinion/gallup/286490/oppose-micro-targeting-online-political-ads.aspx [https://perma.cc/V7RC-DGW9] (finding that 72% of Americans oppose internet companies providing political campaigns access to user data for microtargeting—a view shared roughly equally by Republicans (75%), independents (72%), and Democrats (69%) alike).

Facebook would have the duty to ensure that their preferences are respected, and that political advertisers are not misappropriating their personal data. For users that choose to stick with the status quo, Facebook would be required to respect their preferences as well. Facebook would already be in violation of its duty of care, given that its ad-delivery system—even when advertisers input identical targeting parameters—preferentially delivers ads to users deemed most "relevant."[272] Facebook would have a duty not only to fix its algorithms so that political ads are no longer delivered to users in a biased fashion, but also to continuously monitor its algorithms through yearly or bi-yearly internal audits. Finally, Facebook would have a duty to warn users about potentially false or misleading political ads. Facebook's policy during the 2020 election of labeling *all* posts related to mail-in voting with a message about how to receive official voting information was not the same as warning users.[273] To satisfy its duty of care, Facebook must flag the *specific* posts that are potentially false or misleading to protect its users from the growing threat of voter suppression in future elections.

Under the duty of loyalty, Facebook would be required to prioritize the interests of its end users, even if that means deviating from its current business model. Efforts to warn users about the dangers of political microtargeting would likely affect Facebook's bottom line, assuming these efforts result in more users opting out of receiving microtargeted political ads. Facebook would be required to honor the microtargeting preferences of its users regardless of the financial consequences. Such fiscal consequences would be warranted given the government's legitimate interest in promoting electoral integrity, representing a new cost of doing business.

Finally, under the duty of confidentiality, Facebook would be obliged to maintain the trust and confidence of its end users by not sharing their personal data with third parties without their informed consent. The Cambridge Analytica scandal constituted a massive breach of Facebook's duty of confidentiality, as Facebook allowed a third party—Cambridge Analytica—to access data from up to eighty-seven million Facebook users without their consent.[274] Facebook must only use end-user data for political microtargeting if it has been explicitly authorized to do so.

Courts would likely analyze whether imposition of these fiduciary duties is a "regulation[] of professional conduct that incidentally burden[s] speech."[275] Any burdens imposed on the speech of political advertisers would be plainly incidental to the legislation's primary goal of regulating online

---

[272] *See* Ali et al., *supra* note 101.

[273] *See* Sheth, *supra* note 52.

[274] *See* Kang & Frenkel, *supra* note 42.

[275] NIFLA v. Becerra, 138 S. Ct. 2361, 2373 (2018).

platforms' handling of end-user data and should, therefore, pass constitutional muster. In sum, treating Facebook as an information fiduciary would mean holding Facebook to the same duties of care, loyalty, and confidentiality that make up the traditional fiduciary relationship. Subjecting Facebook and other digital platforms to this information-fiduciary standard would both mitigate the negative effects of political microtargeting that plague the speech environment on social media, as well as promote electoral integrity in our digital age.

B. The Broader Applicability to Targeted Commercial Advertising

The information-fiduciary approach is applicable with equal force in the commercial-advertising context. Digital companies would need to similarly restructure their websites to ensure that customers are providing their *informed* consent when choosing not to opt out of receiving targeted commercial ads. These companies must provide their consumers with *adequate* notice about how targeted commercial advertising can lead to algorithmic discrimination and consumer manipulation, [276] and with *meaningful* choice over how to receive commercial ads. As information fiduciaries, these companies would also be expected to abide by the duties of care, loyalty, and confidentiality when handling customer data. Federal legislation imposing fiduciary duties on online service providers would greatly bolster consumer protections, resolving Professors Khan and Pozen's concern about the problems inherent in targeting advertising business models.

CONCLUSION

Professors Lina Khan and David Pozen directly challenged supporters of the information-fiduciary model to demonstrate why it is a promising path forward. This Note has taken them up on this challenge, illustrating how Professor Balkin's information-fiduciary approach would mitigate the risks of political microtargeting on digital platforms. Recognizing the limitations of Professor Balkin's proposal, this Note advocates for the passage of federal legislation that would instill online service providers with fiduciary duties toward their end users that trump any duties owed to their shareholders. This Note outlines what enforcement of these duties would look like in the particular context of political microtargeting on Facebook, while also providing a model for their application in the context of targeted commercial advertising more broadly. And, most importantly, this Note demonstrates that treating digital platforms as information fiduciaries reconciles data

[276] *See* sources cited *supra* notes 19–26 and accompanying text.

privacy with the First Amendment, offering a promising path forward for responding to some of the most pressing challenges of our digital age.

Today, as our nation grapples with one of the worst public-health crises in modern history and the tumultuous aftermath of the 2020 presidential election, the stakes for data-privacy reform have never been higher. Misinformation surrounding COVID-19, as well as the results of the election, has sown doubt and division across the American populace, threatening to tear apart the social fabric of our country. The attempted coup at the U.S. Capitol—an unprecedented assault on American democracy—epitomizes the fateful consequences that can arise when conspiracy theories and mistruths are able to spread unchecked on digital platforms.[277] Therefore, online service providers have a heightened responsibility to ensure that the data of their end users is protected, not exploited by nefarious actors. If there were ever a time for designating online service providers as information fiduciaries, it is now.

[277] Amanda Seitz, *Mob at U.S. Capitol Encouraged by Online Conspiracy Theories*, AP NEWS (Jan. 7, 2021), https://apnews.com/article/donald-trump-conspiracy-theories-michael-pence-media-social-media-daba3f5dd16a431abc627a5cfc922b87 [https://perma.cc/HK5U-WZKQ].