2019

Marketplace of Ideas, Privacy, and the Digital Audience

Alexander Tsesis

MARKETPLACE OF IDEAS, PRIVACY, AND THE DIGITAL AUDIENCE

*Alexander Tsesis**

The availability of almost limitless sets of digital information has opened a vast marketplace of ideas. Information service providers like Facebook and Twitter provide users with an array of personal information about products, friends, acquaintances, and strangers. While this data enriches the lives of those who share content on the internet, it comes at the expense of privacy.

Social media companies disseminate news, advertisements, and political messages, while also capitalizing on consumers' private shopping, surfing, and traveling habits. Companies like Cambridge Analytica, Amazon, and Apple rely on algorithmic programs to mash up and scrape enormous amounts of online and otherwise available personal data to microtarget audiences. By collecting and then processing psychometric data sets, commercial and political advertisers rely on emotive advertisements to manipulate biases and vulnerabilities that impact audiences' shopping and voting habits.

The Free Speech Clause is not an absolute bar to the regulation of commercial intermediaries who exploit private information obtained on the digital marketplace of ideas. The Commerce Clause authorizes passage of laws to regulate internet companies that monetize intimate data and resell it to third parties. Rather than applying strict scrutiny to such proposed regulations as one would to pure speech, judges should rely on intermediate scrutiny to test statutes limiting the commercial marketing of data.

Legislative reforms are needed to address the substantial economic effects of massive, commercial agglomeration of data files containing histories, daily routines, medical conditions, personal habits, and the like. To address this logarithmically expanding cyberphenomenon, Congress should temporally restrict the retention and trade in private data. Internet intermediaries should not be immune from such a restriction on private data storage. For such a policy to be effective, safe harbor provisions shielding internet intermediaries should be modified to allow for civil litigation against internet companies that refuse a data subject's request to remove personal information no longer needed to accomplish the transaction for which it was originally processed.

---

* Raymond & Mary Simon Chair in Constitutional Law and Professor of Law, Loyola University School of Law, Chicago. Thanks is due and deeply felt for the helpful comments of Felix Wu, Nadia Sawicki, Stephen Rushin, Alexandra Roginsky, Juan Perea, Dawn Nunziato, Helen Norton, Ronald Krotoszynski, Jr., John Inazu, David Han, James Grimmelmann, Caroline Mala Corbin, Alan Chen, Sam Brunson, Joseph Blocher, Ashutosh Bhagwat, Eric Berger, and Enrique Armijo. I am also grateful for the feedback I received at the Yale Law School's Free Expressions Scholars Conference, Notre Dame Law School, and the University of Colorado School of Law.

> *Our own information—from the everyday to the deeply personal—is being weaponized . . . . These scraps of data, each one harmless enough on its own, are carefully assembled, synthesized, traded and sold.*
>
> *Taken to the extreme this process creates an enduring digital profile and lets companies know you better than you may know yourself. Your profile is a bunch of algorithms that serve up increasingly extreme content, pounding our harmless preferences into harm.*
>
> —*Tim Cook, Apple Corp. CEO*[1]

INTRODUCTION

One of the most complex puzzles in constitutional law is how to adjudicate cases where a commercial speaker disseminates private information in the marketplace of ideas without the data subjects' prior consent. This conflict has become particularly acute with the expanding online library of personal information. Internet firms rely on algorithmically powered technologies to sift through enormous amounts of information relevant for monitoring, retailing, convincing, or reselling. Electronic tools enable websites to aggregate consumer information, which can almost instantaneously be commodified and linked to hundreds of thousands of additional data points about consumer information, lifestyle habits, demographics, political preferences, reading habits, travel routes, ambitions, illnesses, and so forth.

Internet intermediaries provide audiences with a wealth of public and private information. They function as gatekeepers relying on well-orchestrated marketing strategies, capable of influencing consumers' experiences,

1 Tim Cook, CEO, Apple Inc., Keynote Address at the 40th International Conference of Data Protection and Privacy Commissioners (Oct. 24, 2018), *quoted in* Natasha Lomas, *Apple's Tim Cook Makes Blistering Attack on the 'Data Industrial Complex,'* TECHCRUNCH (Oct. 24, 2018), https://techcrunch.com/2018/10/24/apples-tim-cook-makes-blistering-attack-on-the-data-industrial-complex/.

behaviors, and thoughts.[2] Commercial speech benefits corporations, and in the internet world it benefits mostly online data providers, as opposed to consumers.[3] Much of the information they obtain through free services, such as email or social platforms, is transmitted to commercial parties not involved in the original electronic transaction. The data subject[4] loses control of information when the internet platform transmits private facts to third parties without the subject's knowledge or approval. This cross-pollination of information directs consumer experiences and political exposure to paid advertisements that can algorithmically profile and target audiences.[5] Even extortionists have found compromising information, such as arrest photographs located on police and news websites, helpful for shaking down subjects.[6] Online intermediaries substantially impact consumer privacy, civic information, and even personal reputations. Marketing in profiles creates opportunities and risks. Internet intermediaries channel information, making it easier to navigate the internet. But users' privacy is compromised when data brokers refuse to divulge to consumers all the online third parties with whom they exchange profiles.

This Article argues that massive retention of personal information poses a substantial harm to the privacy interests of data subjects. Congress should rely on its Commerce Clause authority to regulate internet intermediaries' sales of commercial data. Social media companies enjoy trillions of dollars in profits, having a substantial enough effect on interstate commerce to require federal initiative to control the sale, resale, and analysis of personal informa-

2 CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 147 (2016) ("Internet companies vie to achieve platform status, so that they have a monopoly over the user experience, and thus can monetize and control it.").

3 *See* Kathleen M. Sullivan, *Two Concepts of Freedom of Speech*, 124 HARV. L. REV. 143, 158 (2010) ("While the case was litigated by consumer protection advocates and others seeking to lower drug prices by lowering information costs, corporate speakers soon became the principal beneficiaries of subsequent rulings . . . ." (footnote omitted)); *see also* Julie E. Cohen, *The Zombie First Amendment*, 56 WM. & MARY L. REV. 1119, 1120 (2015); Morgan N. Weiland, *Expanding the Periphery & Threatening the Core: The Ascendant Libertarian Speech Tradition*, 69 STAN. L. REV. 1389 (2017).

4 For the definition of data subject, I am borrowing from the European General Data Protection Regulation. Commission Regulation 2016/679 of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, 2016 O.J. (L 119) 1, 33 [hereinafter GDPR] ("'[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.").

5 *See* Paul Lewis, *'Utterly Horrifying': Ex-Facebook Insider Says Covert Data Harvesting Was Routine*, GUARDIAN (Mar. 20, 2018), https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas.

6 Samantha Schmidt, *Owners of Mugshots.com Accused of Extortion: They Attempted 'to Profit off of Someone Else's Humiliation,'* CHI. TRIB. (May 18, 2018), https://www.chicagotribune.com/business/ct-biz-mugshot-website-owners-extortion-20180518-story.html.

tion tendered for specific digital transactions. The First Amendment does not protect online data collectors, and U.S. law should be modified to establish civil causes of action for publishing defamatory and knowingly misleading information. My focus is on commercial transactions. Thus, the suggested regulations do not apply to natural, private persons processing data. Cyberbusinesses profit from data retention, resale, and algorithmic profiling. Consumer protection laws prohibiting the nonconsensual manipulation of processed personal data are in order in such a marketing scheme.

Reliance on psychometrics about such characteristics as socioeconomic backgrounds benefits marketers.[7] Commercial entities regularly hire specialists to harvest messages, user histories, purchases, social media uses, and other data points useful in identifying idiosyncratic behaviors. An audience's right to information and a subject's right to privacy often clash. The marketplace of commerce is not the same thing as the marketplace of ideas.

In the United States, the Supreme Court tends to favor an audience's right to access, receive, and obtain information,[8] but it recognizes that com-

---

7 d3con, *Cambridge Analytica Explains How the Trump Campaign Worked*, YOUTUBE (May 12, 2017), https://www.youtube.com/watch?v=bB2BJjMNXpA. Psychometrics are data measurements used in advertising for targeted campaigns. Madeline Ford, *What is Psychometrics?*, MOTIVEMETRICS (June 19, 2013), http://blog.motivemetrics.com/What-is-psychometrics. These databases of marketing information include such measures as the data subject's openness, conscientiousness, extroversion, agreeableness, and emotional stability. PAUL KLINE, THE NEW PSYCHOMETRICS: SCIENCE, PSYCHOLOGY AND MEASUREMENT 24 (1998) ("[P]sychometrics is the measurement of psychological traits and characteristics . . . ."); Maria Gester, *Psychometric Advertising in Social Media*, MARIAGESTER (Feb. 21, 2017), http://mariagester.se/2017/02/21/psychometric-advertising-in-social-media/.

8 Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 604 (1982) ("Underlying the First Amendment right of access to criminal trials is the common understanding that 'a major purpose of that Amendment was to protect the free discussion of governmental affairs.'" (quoting Mills v. Alabama, 384 U.S. 214, 218 (1966)); First Nat'l Bank of Bos. v. Bellotti, 435 U.S. 765, 783 (1978) (ruling that "decisions involving corporations in the business of communication or entertainment are based not only on the role of the First Amendment in fostering individual self-expression but also on its role in affording the public access to discussion, debate, and the dissemination of information and ideas"); Red Lion Broad. Co. v. FCC, 395 U.S. 367, 390 (1969) (discussing audience's right to access "social, political, esthetic, moral, and other ideas and experiences"); Lamont v. Postmaster Gen., 381 U.S. 301, 307–10 (1965) (Brennan, J., concurring) (asserting that addressees of mail can challenge seizure); Thomas I. Emerson, *The Affirmative Side of the First Amendment*, 15 GA. L. REV. 795, 807–08 (1981); David S. Han, *The Mechanics of First Amendment Audience Analysis*, 55 WM. & MARY L. REV. 1647 (2014).

On the other hand, in some democracies, such as New Zealand and Australia, the right to "seek, receive, and impart information," opinions, or ideas is not a judicial creation but explicitly protected by statutes. New Zealand Bill of Rights Act 1990, s 14. New Zealand does not have a written constitution. Instead, various laws, such as the Bill of Rights, function as statutory provisions, without the higher law function of the U.S. Constitution. Michael Principe, *The New Zealand Bill of Rights: A Step Towards the Canadian and American Examples or a Continuation of Parliamentary Supremacy?*, 6 FLA. J. INT'L L. 135, 136 (1990). Similarly, section 16(2) of the Australian Human Rights Act of 2004 states: "Everyone has the right to freedom of expression. This right includes the freedom to seek, receive and

mercial communication is of a lower First Amendment value than philosophical, artistic, and scientific expressions.[9] What is more, defamation, which is not uncommon in the digital marketplace, has no value in the quest for truth. Without effective consumer privacy laws, a data subject seeking to remove defamatory statements or videos is at the mercy of companies' opaque review processes. On the internet, the troublesome material can be viewed thousands (even millions) of times.[10] In this Article, my interest is not a philosophical concept of privacy, but more narrowly the principles relevant to consumer privacy protections in the digital realm. Under those circumstances, regulation of commercial digital speech is a substantial government interest that might be narrowly tailored to safeguard details about a person's sexuality, finances, address, and health.

Resolution of audience/privacy conflicts is critical in a marketplace saturated with digital technologies providing invaluable information at the cost of capturing personal details about users. Five companies dominate the digital realm: Amazon, Apple, Alphabet, Facebook, and Microsoft.[11] Each spe-

---

impart information and ideas of all kinds, regardless of borders, whether orally, in writing or in print, by way of art, or in another way chosen by him or her." *Human Rights Act 2004* (Cth) s 16(2) (Austl.).

9 It is important to note here a recent potential shift in the Court's reasoning. Some scholars argue that in *Sorrell v. IMS Health Inc.*, the Court shifted to a content-based approach to commercial speech. 564 U.S. 552 (2011); Paula Lauren Gibson, *Does the First Amendment Immunize Google's Search Engine Search Results from Government Antitrust Scrutiny?*, 23 COMPETITION 125, 136 (2014); Hunter B. Thomson, Note, *Whither* Central Hudson? *Commercial Speech in the Wake of* Sorrell v. IMS Health, 47 COLUM. J.L. & SOC. PROBS. 171, 173 (2013). Their confusion comes from the majority's review in *Sorrell* of something akin to viewpoint discrimination analysis. "[The law at issue] goes even beyond mere content discrimination, to actual viewpoint discrimination." *Sorrell*, 564 U.S. at 565 (quoting R.A.V. v. City of St. Paul, 505 U.S. 377, 391 (1992)). Whatever the trend, for now, the *Sorrell* Court made clear it was sticking with intermediate scrutiny. Specifically, the majority asserted that restrictions on commercial speech cannot be sustained unless they "directly advance[ ] a substantial governmental interest and that the measure is drawn to achieve that interest." *Id.* at 572.

10 One example is a video falsely accusing Broward County Sheriff Scott Israel of heinous acts, including rape. Even though Israel's accuser later denounced the claim, admitting that she was paid to make the false video, YouTube refused to take the data off its platform. Marc Caputo, *'Oh My God . . . It's Fake': Far Right Falls for Hoax About Broward County Sheriff*, POLITICO (Mar. 23, 2018), https://www.politico.com/story/2018/03/23/florida-school-shooting-sheriff-hoax-482170.

11 *See* Andy Greenberg, *How One of Apple's Key Privacy Safeguards Falls Short*, WIRED (Sept. 15, 2017), https://www.wired.com/story/apple-differential-privacy-shortcomings/; *Lawsuit Accuses Google of Stealing Data of 5m UK Users*, PHYS.ORG (Nov. 30, 2017), https://phys.org/news/2017-11-lawsuit-accuses-google-5m-uk.html; Shannon Liao, *Google Admits It Tracked User Location Data Even When the Setting Was Turned Off*, VERGE (Nov. 21, 2017), https://www.theverge.com/2017/11/21/16684818/google-location-tracking-cell-tower-data-android-os-firebase-privacy; Natasha Lomas, *A Closer Look at the Capabilities and Risks of iPhone X Face Mapping*, TECHCRUNCH (Nov. 4, 2017), https://techcrunch.com/2017/11/04/a-closer-look-at-the-capabilities-and-risks-of-iphone-x-face-mapping/; Farhad Manjoo, *Tech's Frightful Five: They've Got Us*, N.Y. TIMES (May 10, 2017), https://www.nytimes.com/

cializes in the development and manipulation of technologies designed to provide data to targeted audiences while tracking details about everything from people's employment history, to their race, police records, gender, sexual preference, addictions, and anything else that will help to algorithmically improve marketing. Benefitting from customers' personal data and reselling does not fit the traditional marketplace of ideas model; rather, it is a commercial scheme to profit corporations, not natural persons. To listen to the former Google CEO, Eric Schmidt, one would think social media forums are altruistic entities gathering public and intimate portraits of online users to best benefit their audiences:

> With your permission you give us more information about you, about your friends, and we can improve the quality of our searches. We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about.[12]

In the name of improving product quality and delivery, Schmidt apparently thinks marketing can be done by all-knowing corporations providing commercial services. But the practice of corporate officers automatically destroying their email on their own servers and other account holders' inboxes demonstrates that Facebook and others know full well the value of privacy but provide customers with fewer safeguards than they rely on.[13]

2017/05/10/technology/techs-frightful-five-theyve-got-us.html; Jack Morse, *Apple's TrueDepth Camera Will Be Used to Send Face Data to Third Parties*, MASHABLE (Nov. 2, 2017), https://mashable.com/2017/11/02/apple-iphonex-faceid-truedepth-privacy-ad-tracking/#TrKpmLeRHsqu; Mike Sands, *Customer Data Is the Secret to Silicon Valley's Success*, FORBES (Nov. 29, 2017), https://www.forbes.com/sites/mikesandsl/2017/11/29/customer-data-is-the-secret-to-silicon-valleys-success/#19fc551a6c3b; Nick Statt, *Amazon Will Let Alexa Developers Use Voice Recognition to Personalize Apps*, VERGE (Nov 28, 2017), https://www.theverge.com/2017/11/28/16711134/amazon-alexa-echo-voice-recognition-developers-personalize-apps; Mark van Rijmenam, *How Amazon Is Leveraging Big Data*, DATAFLOQ (Jan. 23, 2013), https://datafloq.com/read/amazon-leveraging-big-data/517; Tom Warren, *Microsoft Finally Reveals What Data Windows 10 Really Collects*, VERGE (Apr. 5, 2017), https://www.theverge.com/2017/4/5/15188636/microsoft-windows-10-data-collection-documents-privacy-concerns; Robert Williams, *Apple Shares Facial Recognition Data with Apps, Sparking Privacy Worries*, MOBILE MARKETER (Dec. 1, 2017), https://www.mobilemarketer.com/news/apple-shares-facial-recognition-data-with-apps-sparking-privacy-worries/512048/.

12 ADAM HODGKIN, FOLLOWING SEARLE ON TWITTER: HOW WORDS CREATE DIGITAL INSTITUTIONS 185 (2017) (quoting Eric Schmidt, former CEO of Google).

13 Facebook's founder Mark Zuckerberg is laughing to the bank about people's gullibility of giving him monetizable, personally identifiable information. "In 2010, Silicon Alley Insider . . . published now-infamous instant messages from a 19-year-old Zuckerberg to a friend shortly after starting The Facebook in 2004. 'yea so if you ever need info about anyone at harvard . . . just ask . . . i have over 4000 emails, pictures, addresses, sns' Zuckerberg wrote to a friend. 'what!? how'd you manage that one?' they asked. 'people just submitted it . . [.] i don't know why . . . they "trust me" . . . dumb fucks' Zuckerberg explained." Josh Constine, *Facebook Retracted Zuckerberg's Messages from Recipients' Inboxes*, TECHCRUNCH (Apr. 5, 2018), https://techcrunch.com/2018/04/05/zuckerberg-deleted-messages/.

Facebook's mission statement[14] similarly presents a company seeking to benefit consumers, and it is truly a remarkable platform for bringing family, friends, and strangers together. It has the ability to spread cultural richness of immense importance to the spread of political and commercial ideas. But consumers rarely understand how extensively social media companies share personal data with third parties without data subjects' consent. Social media terms-of-service contracts typically ask the public to surrender all their data for analysis and resale, but the language is typically hidden in the midst of documents full of legalese.[15] These can be understood by lawyers, but for the general public, the terms of service are ambiguous, uncertain, and can be unilaterally modified. A Berlin court agreed with the plaintiff's claim that, "Facebook hides default settings that are not privacy-friendly in its privacy center and does not provide sufficient information about it when users register."[16] Google can indefinitely retain personal information, including video, audio, purchases, and activity on third-party sites using that company's services.[17] Even newspapers like the *New York Times* sell to and purchase from third parties such data subject details as demographics, including "age, sex, household income," and similar metrics.[18] The newspaper uses the information both to isolate personality traits to determine content preferences and to anonymize data to conduct largescale studies.[19] While digital advertisement superficially resembles traditional marketing, the two are significantly differ-

14 "Facebook's mission is to give people the power to build community and bring the world closer together." *FAQs: What is Facebook's Mission Statement?*, FACEBOOK: INVESTOR RELATIONS, https://investor.fb.com/resources/default.aspx (last visited Feb. 20, 2019).

15 Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 697 (2013) ("[E]vidence suggests that many users of Facebook do not understand how their privacy settings work in practice."); Mark Daniel Langer, Note, *Rebuilding Bridges: Addressing the Problems of Historic Cell Site Location Information*, 29 BERKELEY TECH. L.J. 955, 970 n.118 (2014) (reporting that "when Google and Facebook updated their privacy policies in 2012, a survey found that the changes to the policies were too confusing for customers to understand"); Alison C. Storella, Note, *It's Selfie-Evident: Spectrums of Alienability and Copyrighted Content on Social Media*, 94 B.U. L. REV. 2045, 2080 (2014) (stating, based on studies, that "many users simply do not know or understand how social media privacy settings work").

16 *German Court Finds Facebook Guilty of Privacy Violations*, DEUTSCHE WELLE (Feb. 12, 2018), https://www.dw.com/en/german-court-finds-facebook-guilty-of-privacy-violations/a-42553867; *see also Facebook Broke German Privacy Laws, Court Rules*, BBC NEWS (Feb. 12, 2018), https://www.bbc.com/news/technology-43035968 (explaining that the German court found Facebook's preclick policy to be insufficient for providing consumers notice). Privacy statements from private corporations, like Facebook, to newspapers, like the *New York Times*, allow social media companies to gather large swaths of information, including age, sex, household income, job industry, and job title. *See Data Policy*, FACEBOOK, https://www.facebook.com/policy.php (last visited July 2018).

17 *Google Privacy Policy*, GOOGLE, https://policies.google.com/privacy?hl=en#infocollect (last visited July 2018) (listing information Google collects).

18 *Privacy Policy* § 1.B, N.Y. TIMES, https://help.nytimes.com/hc/en-us/articles/11501492108-Privacy-policy#1 (last updated May 24, 2018).

19 *Id.* § 2.

ent because the latter is able to capture data users' profiles, not only inform them with useful information.

With precious few regulations in the United States governing their business strategies, internet intermediaries monetize user profiles by capturing private data information through tracking digital tools and artificial intelligence. Personalized data points are monetized either by direct marketing or sales to digital third parties. Without legal guidelines, social media companies use opt-in options for controlling, retaining, and exchanging private information. Facebook has been a master of exploiting such data: a tech journalist found that by creating an account, she activated numerous public settings:

> [H]ere's everything that was public or turned on by default: My friends list. My profile, which could be indexed by search engines. I could be tagged in any post, even if I hadn't reviewed it first. The site would suggest that my friends tag me in images. Ad targeting would let Facebook sell marketers the ability to find me based on my relationship status, employer, job title, education and interests. And Facebook would use my app and browser activity to decide which ads to show me.[20]

Without clearly consenting to the spread of data, and without even knowing who is receiving them, the user's profile is commodified. Social media companies are not covered by privacy rules, such as those that apply to healthcare organizations under Health Insurance Portability and Accountability Act.[21] A consumer seeking ideas in the marketplace should enjoy greater autonomy to consent about their choice of services, rather than give up virtually their entire bundle of privacy to curious audiences. The European Union relies on opt-in automation, while in the United States the default option is opt-out. The latter puts the onus on consumers, rather than exercising an interstate plan of fair dealing and consumer protections.

While the Supreme Court tends to favor speakers' rights to explore ideas, no provision of the Constitution provides a hierarchy of preferences when a natural data subject has privacy interests that are detached from the typical online data providers' business model. As against the subjects' right to maintain control over private matters, corporate purpose is chiefly profit from sales to third parties of data bits saturated with personal information that is digitized and algorithmically analyzed.[22] In those circumstances, judg-

---

20 Staci D. Kramer, *Facebook Could Easily Make Privacy the Default. It Still Hasn't*, WASH. POST (Apr. 11, 2018), https://www.washingtonpost.com/news/posteverything/wp/2018/04/11/i-tested-facebooks-privacy-settings-theyre-worse-than-zuckerberg-says/?utm_term=.fb00dc199237.

21 *See, e.g.*, 45 C.F.R. § 160.102 (2018); Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 434, 441–43 (2018).

22 I am thinking of the penumbral privacies such as it is established in *Griswold v. Connecticut*. 381 U.S. 479 (1965). In that decision, Justice Douglas demonstrates that there is a privacy that is the backbone of several constitutional provisions, including the First Amendment, Fourth Amendment, and Ninth Amendment. *Id.* at 484. More recent cases, such as *Roe v. Wade*, ground privacy in Fourteenth Amendment doctrine. 410 U.S. 113, 153 (1973). But the Court has never outright overturned Justice Douglas's penumbral

ment must be contextual and balanced without deviating from the singularity of speech as a transmitter of information and privacy as a dignitary interest. Both speech and privacy are protected constitutional interests, and in combination they advance individual and social concerns. Both speech and privacy are crucial to the exercise of personal autonomy and the enjoyment of privileges common to all members of a representative democracy.[23] Personal autonomy involves meaningful commercial and political choices. Privacy and speech are separate topics, but in the digital world articulating their connection is important for deciding when regulatory restrictions on speech benefit the general welfare by preserving private integrity.

The First Amendment protects both speakers' abilities to spread ideas[24] and audiences' access to information.[25] Neither the rights of a speaker nor those of an audience are unlimited entitlements,[26] but both the right of expression and the right to acquire information are tied to the Amendment's overall function to protect the people's articulation of political messages, personal expressions, and scientific or artistic participation.[27] Quite often information sought by one segment of the audience is guarded by individuals who want it out of the public eye.

This Article argues that, in cases where audience rights and privacy rights conflict, only a holistic constitutional analysis can explain why some forms of content—copyright[28] and antitrust laws,[29] as just two examples—are not protected by the First Amendment: judges should not limit themselves to the needs of the marketplace of ideas. In today's linked world, privacy needs

---

analysis in *Griswold*. I hope, dear reader, that you will understand that in an article of this length I am unable to expostulate on this admittedly controversial point of view.

23 Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 124–33 (2004) (discussing "privacy in terms of 'contextual integrity'").

24 Consol. Edison Co. v. Pub. Serv. Comm'n, 447 U.S. 530, 541–42 (1980) ("Where a single speaker communicates to many listeners, the First Amendment does not permit the government to prohibit speech as intrusive unless the 'captive' audience cannot avoid objectionable speech.").

25 Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 567 (1980) (asserting that "the suppression of advertising reduces the information available for consumer decisions and thereby defeats the purpose of the First Amendment").

26 *See, e.g.*, Branzburg v. Hayes, 408 U.S. 665, 684 (1972) ("It has generally been held that the First Amendment does not guarantee the press a constitutional right of special access to information not available to the public generally.").

27 Alexander Tsesis, *Free Speech Constitutionalism*, 2015 U. ILL. L. REV. 1015, 1027–42.

28 Golan v. Holder, 565 U.S. 302 (2012).

29 *See* Frederick Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 HARV. L. REV. 1765, 1768 (2004) ("Little case law and not much more commentary explain why the content-based restrictions of speech in the Securities Act of 1933, the Sherman Antitrust Act, the National Labor Relations Act, the Uniform Commercial Code, the law of fraud, conspiracy law, the law of evidence, and countless other areas of statutory and common law do not, at the least, present serious First Amendment issues."); Melanie K. Nelson, Comment, *The Anticompetitive Effects of Anti-Abortion Protest*, 2000 U. CHI. LEGAL F. 327, 363.

often conflict with the profitmaking interests of social media audiences.[30] Digital transactions should be tested by evaluating speakers' interests, consumer protections, regulatory fit to policies, precision in drafting, and relevant doctrines.

The Court's treatment of audiences' interests varies depending on context. In cases of political campaign expenditures, which serve to inform listeners, regulations are subject to "the exacting scrutiny applicable to limitations on core First Amendment rights of political expression."[31] However, only rational basis review applies when government authorities prohibit the dissemination of information in cases of insider trading[32] or blackmailing.[33] Intermediate balancing continues to govern commercial transactions. Where controversies involve more than one constitutional value, the judiciary should weigh evidence tending to support a hearer's demand for information and countervailing concerns about matters like intellectual property, financial markets, consumer privacy, and national security. In addition, courts should protect interests of data subjects to maintain control of their online records against the corporate uses of digital data no longer needed for the purpose for which it was originally generated.

Given the commercial magnitude of the secretive corporate sales of data,[34] the judiciary can only provide part of the solution. Congress should pass a statute pursuant to its Commerce Clause authority. It should also modify the safe harbor provision of the Communications Decency Act, allowing for civil liability of social media platforms that facilitate the dissemination of false and deceptive marketing. In addition, new statutory limitations should be placed on the length of retention and the clandestine commercial dissemination of consumer information.

The Article proceeds as follows: Part I introduces the First Amendment's protections of the marketplace of ideas. Special attention is given to commercial speech doctrine. Part II looks at the erosion of privacy as a result of internet companies harvesting enormous data sets to create psychometric profiles. Profits are thereby gained, affecting interstate commerce with nominal benefits to the marketplace of ideas. Part III, then, discusses the delicate balance between an audience's right to gain beneficial information and an

30 Gregory P. Magarian, *Forward into the Past: Speech Intermediaries in the Television and Internet Ages*, 71 OKLA. L. REV. 237, 251 (2018) ("In contrast to the Television Age, . . . the new speech intermediaries' profitmaking function dominates their social-structuring function.").

31 McCutcheon v. FEC, 572 U.S. 185, 197 (2014) (quoting Buckley v. Valeo, 424 U.S. 1, 44–45 (1976) (per curiam)).

32 SEC v. Lipson, 278 F.3d 656, 664 (7th Cir. 2002) (holding that the imposition of the maximum civil penalty for insider trading was not a violation of the First Amendment); Henry N. Butler & Larry E. Ribstein, *Corporate Governance Speech and the First Amendment*, 43 U. KAN. L. REV. 163, 202 (1994).

33 Robinson v. Jacksonville Shipyards, Inc., 760 F. Supp. 1486, 1535 (M.D. Fla. 1991); C. EDWIN BAKER, HUMAN LIBERTY AND FREEDOM OF SPEECH 60–65 (1989).

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

individual's right to control personal data. It argues that consumer protections are necessary where commercial entities harvest personal data for commercial purposes. However, in cases challenging restraints on political advertisements, courts should require a higher burden of proof to better smoke out censorship. Part IV proposes regulatory reforms to limit the duration for which internet intermediaries can retain and market personal data. It argues that social media firms should not be immune from litigation when they knowingly spread false commercial or political information.

I. AUDIENCES AND DIGITAL COMMERCIALIZATION

Digital audiences' right to access information available in the marketplace of ideas often conflicts with a subject's right to privacy. In *Cox Broadcasting Corp. v. Cohn*, the Court asserted: "In this sphere of collision between claims of privacy and those of the free press, the interests on both sides are plainly rooted in the traditions and significant concerns of our society."[35] Audience-based protections are of paramount importance in disseminating "social, political, esthetic, moral, and other ideas and experiences."[36] The Supreme Court first recognized a First Amendment audience right to receive information in 1965.[37] The freedom to speak implies the right to have free and equal access to ideas and information.[38] Audience access to information is key to the very purpose of the First Amendment—to protect the free flow of opinions and ideologies. The U.S. Supreme Court has recognized audiences' right to access in matters as diverse as investigative journalism of trials[39] and controversial political literature.[40] So too, in the campaign financing area, the Court has articulated audiences' right to obtain useful information for arriving at political decisions.

Political, personal, or informational messages have constitutional meaning, in part, because of their semantic or emotive value to an audience. But audience rights are not absolute. Not all materials advance the marketplace of ideas' quest for truth; in particular, as the Supreme Court has recognized, when data are compiled from multiple sources, they are likely to contain mistakes and misrepresentations.[41]

---

35 Cox Broad. Corp. v. Cohn, 420 U.S. 469, 491 (1975).

36 Red Lion Broad. Co. v. FCC, 395 U.S. 367, 390 (1969).

37 Lamont v. Postmaster Gen., 381 U.S. 301 (1965); *see also* John C. Jeffries, Jr., *Damages for Constitutional Violations: The Relation of Risk to Injury in Constitutional Torts*, 75 VA. L. REV. 1461, 1479 (1989) (listing early right-to-receive-information cases); Burt Neuborne & Steven R. Shapiro, *The Nylon Curtain: American's National Border and the Free Flow of Ideas*, 26 WM. & MARY L. REV. 719, 719 n.139 (1985) (same).

38 Stanley v. Georgia, 394 U.S. 557, 564 (1969) ("[T]he Constitution protects the right to receive information and ideas.").

39 *See* Gannett Co. v. DePasquale, 443 U.S. 368 (1979).

40 *See Lamont*, 381 U.S. at 305.

41 *See* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 752, 780 (1989).

Human interactions in the digital age involve the spread of personal information through computer platforms, such as phones with cameras. Digital conversations, be they through emails or blogs, often trigger targeted marketing in addition to interactions in ideas and a quest for truth. Advertisers embed hyperlinks to give customers the option to connect directly to websites selling products. In addition, corporations adopt a system allowing users to hit a button to demonstrate a visitor's "likes." The number of those favorable ratings is then aggregated. Value is obtained by marketing content to targets who have been algorithmically determined to have a commercial desire to receive and act upon the electromagnetically transmitted material. So-called "friends" are conduits for firms to engage in targeted advertisements, not in some discussion of political or aesthetic values. The most egregious use of this material was Cambridge Analytica's heist of politically manipulable data in the 2016 election.

The implications to consumer privacy are particularly acute in the digital realm. Unlike traditional communicative media, microtechnology allows businesses to indefinitely store private information obtained from direct transactions and third-party dealings.[42] It is unclear the extent to which this gets us to the "truth," as Justice Holmes's marketplace of ideas analogy would have it. Algorithmically obtained information is disseminated based on models created via artificial intelligence outcomes. Tidbits of information are then tagged to create computer profiles based on algorithmic models. Social media companies keep track of people through internet service provider addresses, data acquired through sales, public records, listservs, sharing websites, and so forth. Social media companies invest in technology to boost their profits; any marketplace of ideas advancement from extraction and manipulation of private information is presumed, but no law requires them to prove the likelihood of social or personal benefits. The firms' plans are to paint comprehensive user profiles based on a lifetime of information—to include travel location, commercial preferences, intellectual attributes, racial characteristics, etc.—that can be resold to third-party vendors.[43] As I will elaborate in Part II of this Article, the business strategy of social media networks is to indefinitely retain personal data, not simply to inform the public or individuals of any truth. This commercial intercourse can be regulated because it has a substantial effect on the national economy.

---

42 *See, e.g.*, *Thomson Reuters Privacy Statement*, THOMSON REUTERS, https://www.thomsonreuters.com/en/privacy-statement.html (last visited Mar. 7, 2019). The Thomson Reuters privacy agreement empowers the corporation to store a wealth of highly personal biometric and psychometric data about its clients, including Westlaw users. *Id.*; *see supra* notes 17–18 and accompanying text.

43 For a description of how Internet Protocol addresses are used for transmissions and computer identification, see Alexander Tsesis, *Hate in Cyberspace: Regulating Hate Speech on the Internet*, 38 SAN DIEGO L. REV. 817, 828–29 (2001); Wei-erh Chen, Note, *Optimizing Online Trademark Protections Given the Proliferation of Generic Top Level Domains*, 38 J. CORP. L. 585, 587–88 (2013).

The commercial speech doctrine is predicated on the audience's right to know.[44] However, much online marketing seeks not to inform but to profit by taking "advantage of consumers' cognitive weaknesses and biases."[45] Supreme Court precedents in this area have repeatedly conceived the protection of audiences' access to information to be critical for making good commercial decisions and selecting between advertised products.[46] But where messages aim to influence consumers without appealing to their cognitive, rational faculties, it provides de minimis benefit to the marketplace of ideas.[47]

Social media corporations reap profits by marketing profiles to firms engaged in commercial and political activities. To understand the role of internet marketing it is important to describe the free speech values of advertising. By "commercial speech," the Supreme Court refers to "expression related solely to the economic interests of the speaker and its audience"[48] or "speech proposing a commercial transaction."[49] What is more, commercial speech is valuable for consumer choice and the efficient functioning of a capitalist economy.[50] The commercial nature of advertisements to gain profits distinguishes it from protected explorations of ideas, facts, philosophies, and tastes. Manipulative advertisements are even further afield of protected speech, appealing to emotive responses. The Court therefore only relies on intermediate scrutiny to review restrictions on commercial statements "commensurate with its subordinate position in the scale of First Amendment values, while allowing modes of regulation that might be impermissible in the realm of noncommercial expression."[51] More recently, however, the Court has become increasingly less deferential—some might say increasingly

---

44 Robert Post & Amanda Shanor, Commentary, *Adam Smith's First Amendment*, 128 HARV. L. REV. F. 165, 170 (2015).

45 Micah L. Berman, *Manipulative Marketing and the First Amendment*, 103 GEO. L.J. 497, 522 (2015); *see also id.* at 500 ("Many common advertising techniques do not rely on communicating information, as the Court's commercial speech cases assume that all advertising does. Instead, they seek to influence consumers at a subconscious or emotional level.").

46 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 496–500 (1996); Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 561–63 (1980).

47 Much advertising is emotive; for example, using sexual attraction to sell products. *See* KENT GREENFIELD, THE MYTH OF CHOICE: PERSONAL RESPONSIBILITY IN A WORLD OF LIMITS 59 (2011). Even political advertisement can be emotive, drawing on nationalism, racialism, and class identity. The aim of such advertisement is to mislead and obfuscate. It does not fit the Court's principal justification for constitutional protection of free speech, "the value to consumers of the information such speech provides." Zauderer v. Office of Disciplinary Counsel, 471 U.S. 626, 651 (1985).

48 *Cent. Hudson Gas & Elec. Corp.*, 447 U.S. at 561.

49 *Id.* at 562 (quoting Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978)).

50 *See* Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 763–64 (1976).

51 *Ohralik*, 436 U.S. at 456.

Lochnerian[52]—to consumer protection statutes that limit corporate communications.[53]

While commercial entities benefit from advertising, the Court has explained that a principal value of commercial speech is to enable consumers to receive an array of information.[54] But nothing requires the speech to be exclusively informative or advancing of truth. An advertisement that endorses, encourages, or enthuses is equally protected, even though it does not fit literally into the Court's informational definition. The Court's examination of whether speech is "commercial [in] character" requires judges to examine content, especially when it is "inextricably intertwined with otherwise fully protected speech."[55] In such situations, the Court uses intermediate scrutiny,[56] despite some indication that it might soon move to a more rigorous test in the commercial speech area.[57] There is a possibility that "[r]egulation of a solicitation"[58] might "intertwine[ ] with informative and perhaps persuasive speech."[59] Where audible and visual elements are used to encourage commercial transactions, accuracy is critical to consumers. Misinformation can significantly compromise a buyer's ability to act autonomously as a rational being (in the Aristotelian sense).

The First Amendment safeguards the public's demand for commercial speech to evaluate commodities, and that information is only helpful when it is authentic and truthful. Therefore, false and misleading commercial speech has never been protected and is outside the purview of First Amendment doctrine.[60] Consumers can be victimized by inaccurate devices that lead them to make harmful consumer choices.[61] However, in noncommercial settings, fallacy stated without seeking monetary return is protected.[62] What is important here, as Jack Balkin has pointed out, is the social relation between the communication and the listener. The commercial speech doc-

52 Morton J. Horwitz, *Foreword: The Constitution of Change: Legal Fundamentality Without Fundamentalism*, 107 HARV. L. REV. 30, 109–16 (1993). For arguments that protection of commercial speech revivified *Lochner*-era intrusions into legislative economic prerogatives, see Thomas H. Jackson & John Calvin Jeffries, Jr., *Commercial Speech: Economic Due Process and the First Amendment*, 65 VA. L. REV. 1, 8, 40 (1979).

53 Alexander Tsesis, *The Categorical Free Speech Doctrine and Contextualization*, 65 EMORY L.J. 495, 522 n.169 (2015).

54 Zauderer v. Office of Disciplinary Counsel, 471 U.S. 626, 651 (1985).

55 Riley v. Nat'l Fed'n of the Blind of N.C., Inc., 487 U.S. 781, 796 (1988).

56 *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 566 (1980).

57 *See* Sorrell v. IMS Health Inc., 564 U.S. 552 (2011).

58 *Riley*, 487 U.S. at 796.

59 *Id.* (quoting Village of Schaumburg v. Citizens for a Better Env't, 444 U.S. 620, 632 (1980)).

60 *Cent. Hudson Gas & Elec. Corp.*, 447 U.S. at 566.

61 *See* Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 771–72, 771 n.24 (1976).

62 *See* United States v. Alvarez, 567 U.S. 709, 718–19 (2012); Helen Norton, *Lies and the Constitution*, 2012 SUP. CT. REV. 161, 161.

trine safeguards the right of marketplace consumers of ideas to acquire adequate information to evaluate risks, benefits, and preferences.[63]

Scholars have given various rationales for the protection of commercial speech, but they coalesce around the audience purposes of communicating information that provides truthful details about products and their manufacturers, distributors, or sellers. The visionary scholar on this subject, Martin Redish, has since the early 1970s defended the value of commercial speech on the basis of personal "self-development and self-determination."[64] Commercial speech, as Redish argues, is as empowering as any other form of speech, and treating it differently from other expressions protected by the First Amendment is a form of viewpoint discrimination, which the government is prohibited from undertaking.[65]

That perspective is controversial, and rejected by authors like Robert Post, who believe deliberative democracy is at the core of the First Amendment's protection of free speech. The Court has itself stated that advancing commercial views holds a "subordinate position in the scale of First Amendment values" worthy of only "limited measure of protection."[66] Post opposes conflating libertarian notions of speech with deliberative democracy,[67] although he of course recognizes that modern democracies "must regard their citizens, insofar as they engage in public discourse, as equal and autonomous persons."[68] This leads Post to the illustrative conclusion that seeking "to sell toothpaste" should be regarded differently from communicating and influencing "the formation of democratic public opinion."[69] His analogy resembles then-Justice Rehnquist's, in a dissent, to the effect that the First Amendment concerns "public decisionmaking as to political, social, and other public issues, rather than the decision of a particular individual as to

63 Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1214–16 (2016).

64 Martin H. Redish, *Commercial Speech, First Amendment Intuitionism and the Twilight Zone of Viewpoint Discrimination*, 41 LOY. L.A. L. REV. 67, 81 (2007) [hereinafter Redish, *Commercial Speech*]. *See generally* Martin H. Redish, *The First Amendment in the Marketplace: Commercial Speech and the Values of Free Expression*, 39 GEO. WASH. L. REV. 429 (1971).

65 *See* Redish, *Commercial Speech*, *supra* note 64, at 107.

66 Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978) ("[W]e . . . have afforded commercial speech a limited measure of protection, commensurate with its subordinate position in the scale of First Amendment values, while allowing modes of regulation that might be impermissible in the realm of noncommercial expression.").

Like Post, other scholars attribute a similarly lower view to speech for which the principal or predominant purpose is profit. Frederick Schauer, for instance, writes: "If freedom of speech is based on the interests of the speaker, and if the speaker's dignity or self-respect is the determinative factor, there seems little reason to extend that freedom to those whose only motive is profit." FREDERICK SCHAUER, FREE SPEECH: A PHILOSOPHICAL ENQUIRY 159 (1982).

67 Robert C. Post, *Viewpoint Discrimination and Commercial Speech*, 41 LOY. L.A. L. REV. 169, 175 (2007).

68 Robert Post, *Democracy and Equality*, 603 ANNALS AM. ACAD. POL. & SOC. SCI. 24, 28 (2006).

69 Post, *supra* note 67, at 177.

whether to purchase one or another kind of shampoo."[70] Post nevertheless concedes that it is legitimate to regard commercial speech as an element of information distribution: "Commercial speech does, however, circulate information to the public sphere within which democratic public opinion is formed, and this information might well be relevant to the formation of public opinion."[71] But he does not regard it as having the same First Amendment value as democratic expression.

I would take Post's argument a step further. The First Amendment protects the right of individuals to obtain and circulate information as equal players in a polity whose structure and substantive protections are meant to benefit ordinary people. The First Amendment protects our private and public communicative personalities. To paraphrase Shakespeare's *As You Like It*, all the world is a stage and each of us in his or her time plays many parts. Just as any other cases arising under the First Amendment, challenges to commercial speech regulations require careful analysis of the full context in which statements are made. The Court's decision to treat commercial speech differently from core political speech is content rich.

In the digital age, commercial speech often conflicts with private sensitivities. When private data is commodified without the data subject's consent, privacy should be treated like other commercial speech, under the four-part test from *Central Hudson*. That is, the question for adjudication is whether the speech giving rise to privacy intrusion is lawful or misleading, whether the government has a substantial interest in the privacy regulation, whether the regulation advances important privacy concerns, and whether it "is not more extensive than is necessary to serve that interest."[72] Advertisements can be informative, but in today's digital climate, businesses, especially social media companies, are increasingly relying on the digital methods to sweep up personal information into their databanks without obtaining consumers' explicit permission to do so. Internet intermediaries' privacy statements are often written in such broad language as to license indefinite retention and almost unimpeded commercial exchange in data with third parties.[73] Social media companies also modify their privacy settings without informing users to reconsider their acceptance of terms.[74] The European Commissioner for Justice, Consumers, and Gender Equality, Vera Jourová, issued a statement calling for swift sanctions against Facebook, which like other internet intermediaries, continues to issue "misleading terms of ser-

70 Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 787 (1976) (Rehnquist, J., dissenting).

71 Post, *supra* note 67, at 177.

72 Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 566 (1980).

73 Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 150 (2017) ("The FTC's assumed premise is that an imagined reasonable consumer read a privacy statement and agreed to the terms in it as well as other aspects of a consumer's impressions of the company's privacy representations. . . . The deceptive merchant, then, flouted this reasonable individual's consent. In reality, most consumers do not read privacy policies and are unaware of company's data policies.").

74 PASQUALE, *supra* note 34, at 53, 144–45.

vices" that confuse consumers by obfuscating that its principal corporate purpose is profit.[75] Marketing strategies use the informational model to convince buyers to provide them with a panoply of information that is then stored in databases and sold to a slew of unrevealed third parties or affiliated companies and entities.

II. EROSION OF PRIVACY

Audiences benefit from the wealth of information available on the internet. It is a vast repository containing everything from movies and blogs, to philosophy, medicine, mathematics, law, and engineering, to art and classical studies. Yet it is also a network, where many consumers lack knowledge about how to protect personal data.[76] Digital firms should be required to obtain explicit consent before reselling data information about natural persons. In Europe, privacy is a recognized fundamental right and its enjoyment is significant to the "well-being of individuals."[77] U.S. privacy law, on the other hand, is a patchwork of state-by-state and area-specific federal regulations as well as common-law torts.[78] Greater consumer protections are necessary given the ability of internet firms to gather limitless psychometric details.

Many new gadgets are connected to the internet through operating systems installed in home devices, a marketing strategy collectively known as the

75 *Commissioner Jourová Met with Tech Companies to Push for Full Compliance with EU Consumer Rules*, REPRÉSENTATION AU LUXEMBOURG (Sept. 20. 2018), https://ec.europa.eu/luxembourg/news/commissioner-jourov%C3%A1-met-tech-companies-push-full-compliance-eu-consumer-rules_fr (quoting Commissioner Jourová).

76 *See* Peter Swire, *Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment*, 90 N.C. L. REV. 1371, 1404 (2012); *see supra* note 15 and accompanying text.

77 Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter Directive 95/46/EC].

78 *See, e.g.*, Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422 (2012); Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012) (requiring consumer credit reporting agencies to respect consumers' privacy rights); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2012); Video Voyeurism Prevention Act of 2004, 18 U.S.C. § 1801 (2012); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2012); 18 U.S.C. §§ 2701–2712 (2012) (prohibiting various forms of consumer information compromise by internet and other service providers); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2012); Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–2725 (2012); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C.) (protecting against wrongful disclosure of consumers' private health information); 26 U.S.C § 6103 (2012) (requiring protection of consumer privacy in tax returns); Privacy Protection Act of 1980, 42 U.S.C. § 2000aa (2012); 47 U.S.C. § 230 (2012); Cable Communications Policy Act of 1984, 47 U.S.C. §§ 521–573 (2012) (requiring protection of cable subscriber privacy).

Internet of Things.[79] Household items can now gather psychometrics. Brokers' trade secrets make it impossible for data subjects to trace where that information is disseminated and to whom it has been traded.[80] The inherent biases based on corporate profit in internet search results are undetectable because the algorithms firms have developed are trade secrets.[81] Those secrets only make sense when they improve firms' ability to deliver accurate information to listeners. While internet firms seek to keep their dealings private, they retain unlimited data about their users. Internet-monitoring devices are installed into cell phones, appliances, baby monitoring devices, toasters, ovens, lamps, banks, utilities, security devices, and so on.[82] Appliances with tracking devices gather metrics about the consumer and provide digital marketing companies a huge resource for future advertising and analytics. Much of this deals with commercial transactions, not any effort to get at the truthful information to which Justice Holmes referred to as the marketplace of ideas. Since the dawn of the internet, the default of U.S. internet companies has been to assume that they can make business use of all data acquired because of the opt-out presumption of data protection. This protocol provides inadequate consent about the use of psychometrics like sex, race, gender, sexual orientation, religion, political affiliation, and the like. Data obtained through wired household items can easily be shared because digital companies store it in cloud servers, external to users' physical computers and controls. Emphasis in the United States has been on connectivity with inadequate policy concern placed on privacy and security, allowing for information to be gathered and resold to an unknown number of third-party vendors.[83]

---

79 *See* Jacob Morgan, *A Simple Explanation of 'The Internet of Things,'* FORBES (May 13, 2014), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/; *see also* Laura DeNardis & Mark Raymond, *The Internet of Things as a Global Policy Frontier*, 51 U.C. DAVIS L. REV. 475, 482 (2017) (describing how the Internet of Things raises privacy concerns of corporate and governmental information gathering).

80 *See* Lara Grow & Nathaniel Grow, *Protecting Big Data in the Big Leagues: Trade Secrets in Professional Sports*, 74 WASH. & LEE L. REV. 1567, 1570 (2017) ("[M]ethods of data analysis are most commonly protected under the law of trade secrecy . . . ."); Grant Arnow, Note, *Apple Watch-Ing You: Why Wearable Technology Should Be Federally Regulated*, 49 LOY. L.A. L. REV. 607, 614 (2016) ("Much of . . . 'big data' . . . is collected without consumer awareness and is sold for a variety of commercial purposes."); Meglena Kuneva, Consumer Comm'r, European Comm'n, Speech at the Lisbon Council Event: A Blueprint for Consumer Policy in Europe: Making Markets Work with and for People (Nov. 5, 2009), http://europa.eu/rapid/press-release_SPEECH-09-515_en.htm (stating that the "collection of personal and behaviour data" through technology "is currently being done on an unprecedented scale[,] on a massive scale[,] and mostly without any user awareness at all").

81 *See* Urs Gasser, *Regulating Search Engines: Taking Stock and Looking Ahead*, 8 YALE J.L. & TECH. 201, 232–33 (2006).

82 *See* Andrew Meola, *What Is the Internet of Things (IoT)? Meaning & Definition*, BUS. INSIDER (May 10, 2018), https://www.businessinsider.com/internet-of-things-definition.

83 *See* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1379 (2017).

Individuals wishing to link with others freely divulge their own secrets—be they financial or health—through internet intermediaries. While individuals might want to communicate only with a specific or general audience of natural people, corporations are the big gainers of marketing revenue. Commercial advertisers' for-profit aims often feed off consumers' and voters' raw emotions, racial or national identities, shopping preferences, party affiliations, and any other metrics they can gather online.[84] The national economic effect on interstate commerce warrants passage of consumer protection laws requiring consent and limiting the length for which data brokers can retain private consumer information.

The third-party doctrine restricts data subjects' control over information they have divulged to other parties, be they banks[85] or telephone companies.[86] A subject who uploads information on an interactive internet site exposes himself to the machinations of commercial entities, selling the details to law enforcement agents. Prior to 2018, the third-party doctrine did not require law enforcement agents to get a Fourth Amendment warrant to obtain data that had been divulged to a commercial entity.[87] Data voluntarily tendered to internet companies had been subject to only a police subpoena.[88] After the 2017 Supreme Court term, however, state power has been somewhat curtailed. The third-party doctrine, nevertheless, continues to define the extent to which consumers have reasonable expectations that third parties secure financial and caller information. This doctrine created an end run around for law enforcement agencies circumventing the Fourth Amendment warrant requirements. It continues to limit data subjects' retention of exclusive power to consent to whom private information, especially banking and telephone records, can be sold.

In 2018, the Supreme Court limited the reach of the third-party doctrine. In *Carpenter v. United States*, the Court held that the Fourth Amend-

84 *See* Yoav Hammer, *Expressions Which Preclude Rational Processing: The Case for Regulating Non-Informational Advertisements*, 27 WHITTIER L. REV. 435, 437 (2005); Tamara R. Piety, *"Merchants of Discontent": An Exploration of the Psychology of Advertising, Addiction, and the Implications for Commercial Speech*, 25 SEATTLE U. L. REV. 377, 406 (2001).

85 *See* United States v. Miller, 425 U.S. 435, 444 (1976).

86 *See* Smith v. Maryland, 442 U.S. 735, 741, 743–44 (1979); *see also* Bartnicki v. Vopper, 532 U.S. 514 (2001) (finding that rebroadcast of a matter of public importance did not violate wiretap laws prohibition, where defendants played no role in the initial, illegal interception).

87 For an article written at a time when *Smith* gave key insight into internet communications, see Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 3 (2013) ("Because Internet communications are also voluntarily disclosed to machines in the form of ISPs, arguably under *Smith* users appear to lose any Fourth Amendment protection in these communications. The government would therefore be constitutionally free to acquire these communications from the third-party service provider without first obtaining a warrant, and to use the information against a person at trial." (footnote omitted)).

88 *See* Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 443 (2014); Christine S. Scott-Hayward et al., *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 21 (2015).

ment requires a state to get a search warrant before gaining access to seven days' worth of cell phone site data that law enforcement agents had used for a criminal investigation.[89] "Allowing government access to cell-site records contravenes that expectation [of privacy]," as the Court put it, because it "provides an all-encompassing record of the holder's whereabouts."[90] The Court was keenly conscious of evidence that "seismic shifts in digital technology" required some limit on government's ability to clearly surveil an individual to so great an extent as to breach his "reasonable expectation of privacy in the whole of his physical movements."[91] As Chief Justice Roberts continued for the majority, wireless carriers "are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible."[92]

Carpenter thereby significantly limited the reach of the third-party doctrine. Whereas before, challenges to voluntary conveyance of data from a third party to law enforcement required no Fourth Amendment analysis,[93] after *Carpenter* voluntary disclosures "reduce[ ] expectation[s] of privacy in information knowingly shared with another" but do not eliminate it.[94] The Court contextually analyzed how voluntarily provided data that was used to trace nearly all of an individual's whereabouts for days was distinct from that which a customer divulged to a bank or telephone company. In the words of the majority, "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today."[95] Virtually ubiquitous internet monitoring is very different from single-business record keeping of customer transactions.

Despite *Carpenter*'s benefits to personal privacy against law enforcement infringements, social media companies' transmissions from one private company to another are unaffected by that case because the Fourth Amendment applies only to state actors.[96] So, private third-party transactions remain open to infinite commercial trades in personal data. The right of audiences to access information, therefore, affects subjects beyond the realm of law enforcement, where the Fourth Amendment is relevant.

Social media companies profit by selling user profiles, revealing everything from the users' intimate relations to their sex and race.[97] Consumers reveal information in the first place expecting benefit—socially, professionally, recreationally, and so on—and indeed targeted ads help them do just

89 Carpenter v. United States, 138 S. Ct. 2206 (2018).

90 *Id.* at 2217.

91 *Id.* at 2219.

92 *Id.*

93 *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 442 (1976).

94 *Carpenter*, 138 S. Ct. at 2219.

95 *Id.*

96 *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

97 Nicole A. Ozer, *Facebook Not as Private as You Might Think*, ACLU N. CAL. (Aug. 28, 2007), https://www.aclunc.org/blog/facebook-not-private-you-might-think.

that. But the content is not always of interest to the consumer. Regardless, advertisers pay data brokers whether or not a third-party sale is consummated.[98] Distribution of commercially valuable data to third parties is routinely done without notice to data subjects. Third-party brokers—be they book sellers, toy companies, political parties, or an infinite number of other internet information companies involved in trading data—artificially obtain global permission from data subjects by using privacy statements allowing them to sell the data to anyone. Notice is typically hidden in legal agreements of service, difficult to understand even for experts. Data subjects are given no transparency about data firms' marketing strategies for sharing or otherwise analyzing personal information.[99] Companies seek endorsements in the forms of likes and shares that are not meant to spread factual information but rather are strategic marketing, the contours and nuances of which are hidden beneath layers of proprietary protections.[100]

On the other hand, data brokers and their operating officers seek to keep their own informational privacy, in such matters as trade secrets, while harvesting consumer information. Augmenting their ability to profile, social media companies also purchase other companies' records. For instance, Facebook tracks nearly 30,000 demographic facts, most of which come directly from its platform and others from other data brokers.[101]

Web-based businesses share a wealth of information with other entities, purportedly in the interest of consumers and audiences, without maintaining transparent policies for providing consumers with autonomous control of information.[102] Google searches "deep packet" content of emails and thereby extracts intimate information to use in advertisements and other profitable endeavors.[103] Running sophisticated algorithms enables the com-

98 *See* Jury Demand, Hines v. Openfeint, Inc., 2011 WL 2471471 (N.D. Cal. June 22, 2011) (No. CV113084) (alleging "victims of privacy violations, and unfair and deceptive business wherein their privacy and security rights were violated" in a class action lawsuit); *In re* Google Android Consumer Privacy Litig., 802 F. Supp. 2d 1372, 1373 (J.P.M.L. 2011) (consolidating six causes of action of alleged victims of "improper business practices [that] violated users' privacy by using and sharing plaintiffs' data without authorization").

99 *See 'Act Now, Apologize Later': Will Users 'Friend' Facebook's Latest Intrusion on Privacy?*, KNOWLEDGE@WHARTON (May 12, 2010), http://knowledge.wharton.upenn.edu/article/act-now-apologize-later-will-users-friend-facebooks-latest-intrusion-on-privacy/.

100 Vauhini Vara, *Facebook's Targeted Ads Expand to the Web*, NEW YORKER (Sept. 30, 2014), https://www.newyorker.com/business/currency/facebook-targeted-ads-raise-new-privacy-questions.

101 Alexandra Burlacu, *Facebook Knows a Lot About Your Offline Habits, Buying Third-Party Data to Serve Better Targeted Ads*, TECH TIMES (Dec. 31, 2016), https://www.techtimes.com/articles/190902/20161231/facebook-knows-a-lot-about-your-offline-habits-buying-third-party-data-to-serve-better-targeted-ads.htm.

102 *See* Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 22 (2011).

103 M. Ryan Calo, Essay, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1152 (2011). There is yet no indication that Google has undertaken to desist from deep packet searches; what is more, without regulations even if the firm claimed to do so there would be no way to double-check. What is needed is a reporting regime for internet intermediaries compa-

pany to then send a plethora of related and unrelated materials to the data subject. This has a substantial enough effect on interstate commerce to justify congressional action to better secure personal consumer information. The user is not treated as an autonomous agent but one on whom advertising content can be assigned through computer models. Internet gatekeeping companies, such as Facebook and Alphabet, provide free associational and informational products in exchange for personalized information, making it possible to both electronically deliver them and to thereby acquire advertising revenue. Moreover, the beneficiaries of that data are not only commercial entities: Russia found Facebook and Twitter platforms amenable to its quest of manipulating the 2016 U.S. presidential election, and another company used data available on online platforms to monitor "protest groups and marketed that data to police departments."[104]

Consumers often do not share the interests of commercial data brokers. The Obama administration published a report finding that "when data collected online is combined with data derived from the real world . . . it can cause many kinds of harms, including intrusion into private life, reputational damage, and discrimination against individuals and groups."[105] Of eighty participants in one study, the Pew Research Center found a common frustration of being unable to find out what information internet companies were collecting and what they were sharing with third parties. A revealing comment sums it up: "In my opinion, there is a woeful lack of disclosure on how personal information is used by companies. If you read some of the terms of service, you are essentially giving the company the right to do almost anything with your personal information."[106]

Monitoring tools include Internet Protocol (IP) addresses, cookies, deep packet searches, geolocational technologies, facial recognition processing, and surveillance technologies.[107] As Paul Ohm has pointed out, even if bits

---

rable to the one that exists in the securities area. There are reasons to be skeptical of Google's claim because of its past misleading statements on privacy. For example, the Google corporation misleadingly told users that by turning off the "Location History" function on their Android phones, they would not be tracked, but Google did not divulge that background apps, used by the operating system, continue to track data subjects' whereabouts. *Google Records Your Location Even When You Tell It Not To*, GUARDIAN (Aug. 13, 2018), https://www.theguardian.com/technology/2018/aug/13/google-location-tracking-android-iphone-mobile.

104 Roger McNamee, *How Facebook and Google Threaten Public Health—and Democracy*, GUARDIAN (Nov. 11, 2017), https://www.theguardian.com/commentisfree/2017/nov/11/facebook-google-public-health-democracy.

105 This report is discussed in Jeff Fox, *85% of Online Consumers Oppose Internet Ad Tracking, Consumer Reports Finds*, CONSUMER REP., https://www.consumerreports.org/cro/news/2014/05/most-consumers-oppose-internet-ad-tracking/index.htm (last updated May 27, 2014).

106 LEE RAINIE & MAEVE DUGGAN, PEW RESEARCH CTR., PRIVACY AND INFORMATION SHARING 7 (2016), http://www.pewresearch.org/wp-content/uploads/sites/9/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf.

107 *See* Toby Mendel et al., UNESCO, GLOBAL SURVEY ON INTERNET PRIVACY AND FREEDOM OF EXPRESSION 39–49 (2012).

of explicit identifications—such as name and address—can be removed from online sources, they can later be deanonymized by triangulating indirect user information, such as zip code, birth date, and sex.[108] But the amount of information users divulge goes further. On social networks such as Facebook, Twitter, and Snapchat, users reveal details about their families, love interests, addresses, bosses and employers, political voices, reading preferences, sexual exploits and orientations, health, and infinitely more that allows companies to develop accurate personal portraits. While data subjects often voluntarily post such information on social media sites, none of them can know to whom that information will be sold.[109]

As an example of the intrusiveness involved, Google developed a program for sifting the content of its Gmail service to later convert it into targeted advertisements.[110] Consent was weakly obtained through an overgeneralized privacy statement that did not provide consumers with adequate commercial information about what information the email service was scraping from private emails. Here stringent regulatory privacy standards against deep packet data mining would be in order. Google uses algorithms that are protected by trade secrets to aggregate user information.[111] This makes it impossible to obtain adequate disclosure from firms of how they store, disseminate, and market data.[112] Google's advanced software and algorithms further enable it to gather private information through its Google Chrome browser, which can even record keystrokes entered into the address bar.[113] There are means for reducing the amount of information available to Google, such as disconnecting from the Google Account while searching, but

---

108 Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1719 (2010). For other studies indicating the ease with which research can deanonymize user data using a minimum number of data points from a single or a combination of social media platforms, see Sheera Frenkel, *Scholars Have Data on Millions of Facebook Users. Who's Guarding It?*, N.Y. TIMES (May 6, 2018), https://www.nytimes.com/2018/05/06/technology/facebook-information-data-sets-academics.html.

109 *See* Frenkel, *supra* note 108.

110 *See* JOHN BATTELLE, THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE 194 (2005). Google announced in 2017 that it was phasing out its targeted ads through Gmail, but it will continue to engage in email scanning and recording the content of users' searches, thus continuing to mine personal communications. Daisuke Wakabayashi, *Google Will No Longer Scan Gmail for Ad Targeting*, N.Y. TIMES (June 23, 2017), https://www.nytimes.com/2017/06/23/technology/gmail-ads.html.

111 Editorial, *The Google Algorithm*, N.Y. TIMES (July 14, 2010), https://www.nytimes.com/2010/07/15/opinion/15thu3.html?_r=5.

112 Google and smaller companies like techUK defend the secretive nature of their businesses by arguing that transparency would make their systems more susceptible to hacking and "gaming." *See* Rebecca Hill, *Transparent Algorithms? Here's Why That's a Bad Idea, Google Tells MPs*, REGISTER (Nov. 7, 2017), https://www.theregister.co.uk/2017/11/07/google_on_commons_algorithm_inquiry/.

113 Preston Gralla, *Chrome: Google's Biggest Threat to Your Privacy*, COMPUTERWORLD (Sept. 4, 2008) https://www.computerworld.com/article/2480353/internet/chrome—google-s-biggest-threat-to-your-privacy.html.

the default setting synchronizes Chrome activities with that identifiable account.[114]

Through its trove of personal information, a social media company can harness personal information to contribute to public discourse, and thereby benefit an audience interested in products or politics. However, the information is not simply a matter of objective fact, as one might expect in an ideal marketplace of ideas, where some form of truth would be the aim.

Facebook has tested the limits of users' trust (or perhaps "gullibility" should be the word) by overtly asking for explicit nude photographs, supposedly only to tag the photo to allow the company to prevent others from posting revenge porn with their images.[115] But such a scheme has built-in dangers. Persons might become less wary about posting such videos and photos in the first place, with a plethora of other platforms where they can be posted even if Facebook's platform is not compromised. In addition, hackers could access the images during the transmission from the subjects through internet service providers and onto Facebook.[116] Furthermore, explicit data of sexual organs that the subject would identify might be stolen by Facebook employees. Some regulation of how such data is stored is necessary for consumers to know their data is not abused. Security risks also call for national standards on data storage.

Such a breach of security occurred in other contexts, such as when Google blamed a rogue employee for stealing passwords that the company had acquired clandestinely through software on cars used for the Google Maps project.[117] The company later revealed others knew that personal information was being stolen, showing the lie in the earlier press release.[118] Furthermore, companies like Equifax have lost data in the past and been unable to account for its later dissemination, unable even to say whether it was pilfered by nefarious organizations or individuals.[119]

---

114 Chris Hoffman, *How to Optimize Google Chrome for Maximum Privacy*, How-To Geek (July 12, 2017), https://www.howtogeek.com/100361/how-to-optimize-google-chrome-for-maximum-privacy/.

115 *See* Brett Molina, *Facebook Wants Nude Photos from Australian Users—for a Good Reason*, USA Today (Nov. 8, 2017), https://eu.usatoday.com/story/tech/news/2017/11/08/facebook-tests-fighting-revenge-porn-asking-users-file-nude-photos-first/843364001/.

116 *See* Anthony Cuthbertson, *Why Does Facebook Want Your Nude Photos?*, NewsWeek (Nov. 8, 2017), https://www.newsweek.com/why-does-facebook-nude-photos-revenge-porn-705078; Liz Posner, *Facebook Users Must Decide If They Trust the Social Media Network with Their Nude Selfies*, Salon (Nov. 10, 2017) https://www.salon.com/2017/11/10/facebook-users-must-decide-if-they-trust-the-social-media-network-with-their-nude-selfies_partner/.

117 Emily Anne Epstein & Rob Waugh, *Google Engineers Knew for Two Years That the Company's Street View Cars Were Stealing Emails and Passwords via Wi-fi*, Daily Mail (May 1, 2012), https://www.dailymail.co.uk/sciencetech/article-2137145/Google-KNEW-harvesting-emails-passwords-Street-View-drive.html.

118 *Id.*

119 *See, e.g.*, Brian Feldman, *So What Happens With All That Equifax Data?*, N.Y. Mag.: Intelligencer (Sept. 8, 2017), http://nymag.com/intelligencer/2017/09/so-what-happens-with-all-that-equifax-data.html; Barry Schwartz, *Google Says It Lost 20 Days of Data of New*

Amazon's key service is a further attempt to operationalize a strategy of socializing people to trust online companies with our most intimate information.[120] This one allows the company to deliver not only material products, such as clothes, but also a host of informational materials, including books and CDs. With the key service, Amazon seeks access not just into people's buying habits but into their physical homes. This, along with Amazon's Echo devices and Alexa voice, operated internet services are part of the company's strategy of connecting virtually every aspect of people's lives through the Internet of Things. With Amazon's key service the lock is connected with a cloud camera monitoring the comings and goings of individuals, allowing the home owner to review recorded images but also providing space for Amazon or a hacker to watch the inside of the premises.[121] With this much power being controlled by private firms it is critical for government to step in and create neutral standards for the protection of privacy in a manner designed through the *Central Hudson* standard, protecting speech and weighing countervailing policy that advances important privacy concerns and is no more extensive than is necessary to serve that end.

III. BALANCING AUDIENCE INTERESTS AND PRIVACY CONCERNS

On the one hand, the internet facilitates the spread of ideas; on the other, the same marketing operations affect privacy by the indefinite retention and transaction in personal data. In many cases the more a person knows the better decisions can be made. Firms use that to their advantage through targeted commercial and political advertisements. The internet poses privacy concerns with commercial surveillance not covered by the Fourth Amendment reasonableness requirement for searches and seizures.[122]

The commercial nature of internet business requires judicial oversight, a balancing of concerns for speech and privacy. This is the approach taken in

---

Google Search Console Users, SEARCH ENGINE LAND (July 12, 2017) https://searchengineland.com/google-lost-data-new-google-search-console-users-278708.

120 Selena Larson, *Amazon Key Asks Users to Trade Privacy for Convenience*, CNN (Oct. 26, 2017), https://money.cnn.com/2017/10/26/technology/business/amazon-key-privacy-issue/index.html.

121 *Id.*

122 Riley v. California, 573 U.S. 373, 382 (2014) ("In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement."); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 576 (2009) (demonstrating the importance of third-party doctrine for criminal investigations). For a discussion of how courts have transformed Fourth Amendment doctrine in response to technology, see Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 177 (concluding that Fourth Amendment warrant-level protection is required to safeguard reasonable expectation of privacy); Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433, 458 (2014) ("Some police departments pay cell phone carriers from several hundred to more than two thousand dollars to record and turn over the whereabouts of investigation suspects' cell signals.").

Europe, where judges review laws to decide "whether the means . . . employ[ed] to achieve the aim correspond to the importance of the aim and whether they are necessary for its achievement."[123] In the United States, accurate and informative commercial speech calls for balanced intermediate review,[124] but much of internet content misleads consumers rather than informing them. Internet commercial speech differs from traditional advertising. Typically, commercial speech proposes a commercial transaction.[125] Social media companies do just that. Their proposal for commercial transaction is to provide informational and associational service in exchange for the commodification of private consumer data. The extent to which commercial speech is being used to harvest personal information is unprecedented and requires expanding the definition of commercial speech not only to proposals for commercial transaction but also to commercial transactions that harvest consumers' data for resale to third parties and for algorithmic extraction.

Part III discusses the extent to which consumer privacy is compromised and advocates for judicial review capable of reining in commercial harvesting of unconsented data mining. False political advertisement, however, should be treated differently, subject to the actual malice standard for public officials and traditional libel laws from private parties. This dichotomy recognizes the lower value of commercial speech and the political value of even misleading messages.

A. Commercial Data Exploitation

Contemporary data storage companies hold vast amounts of personal data. Perhaps the foremost of these firms is the giant Acxiom, which as far back as 2009 had 1500 data points "on every American."[126] The company's "database contain[ed] information about 500 million active consumers worldwide."[127] While the human brain forgets, the corporate memory lives on to perpetuity. Firms freely market truthful, credible, pertinent, and useful information. But marketing is not always a transparent art, and it certainly does not always supply useful information as the truth model supposed. Commercial transactions in psychometrics that are based on personality traits (or in technical jargon, "private data") are motivated by profit.[128] Therefore,

123 TAKIS TRIDIMAS, THE GENERAL PRINCIPLES OF EU LAW 139 (2d ed. 2006).

124 Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 573 (1980).

125 Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 761 (1976).

126 Stephanie Clifford, *Ads Follow Web Users, and Get More Personal*, N.Y. TIMES (July 30, 2009), https://www.nytimes.com/2009/07/31/business/media/31privacy.html.

127 Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES (June 16, 2012), https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html.

128 Lyrissa Barnett Lidsky, *Nobody's Fools: The Rational Audience as First Amendment Ideal*, 2010 U. ILL. L. REV. 799, 810 (discussing normative functions of audience protections); Rebecca Tushnet, *Attention Must Be Paid: Commercial Speech, User-Generated Ads, and the Chal-*

the four-part test from *Central Hudson* applies, as it does in all reviews of commercial speech.[129] The same does not hold true for misleading noncommercial speech.

The assumption that audiences can intelligently evaluate information and eventually identify what is truthful is an idealistic presumption that does not bear out in reality.[130] Misleading speech does not even get over the first part of the *Central Hudson* test. In these circumstances, the Supreme Court finds that "[i]f the speech does not pass this preliminary threshold, then it is not protected by the First Amendment at all."[131] Online falsehood can spread broadly and rapidly. Unlike traditional media, Facebook, Twitter, and other services make it easy to create fake accounts that manipulate an audience's access to information and thereby undermine citizens' ability to identify the accuracy of their browsing experiences,[132] further eroding the marketplace of ideas analogy's relevance to misleading internet expression.

On the commercial side, online ads offer links that are created to encourage impulsive purchases, not the well-conceived consumer choices presumed in the commercial speech doctrine.[133] The internet increases the available audience size for savvy marketers, which are not necessarily those with the best-quality or best-priced products. Consumers, therefore, are saddled with adhesive privacy policies, subject to perpetual retention of their data, and given no serious transparency—much less recourse—against social

---

lenge of Regulation, 58 BUFF. L. REV. 721, 730 (2010) ("Given an audience-focused justification for commercial speech doctrine, audiences' dogged attempts to evade or ignore advertising suggest that even if audiences have rights to receive *desired* information that the state would prefer to suppress, such rights can't support an advertiser's claim of a right to provide information in which consumers have expressed no interest.").

129 *Cent. Hudson Gas & Elec. Corp.*, 447 U.S. at 566 ("At the outset, we must determine whether the expression is protected by the First Amendment. For commercial speech to come within that provision, it at least must concern lawful activity and not be misleading. Next, we ask whether the asserted governmental interest is substantial. If both inquiries yield positive answers, we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest."). On the most recent hints of judicial change away from the *Central Hudson* test, see *supra* note 9 and accompanying text.

130 *See* Lidsky, *supra* note 128, at 815 ("[A]ny number of First Amendment doctrines rely on a model of the audience as rational, skeptical, and capable of sorting through masses of information to find truth.").

131 City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 434 (1993).

132 *See* Andrew Hasty, Note, *Treating Consumer Data Like Oil: How Re-framing Digital Interactions Might Bolster the Federal Trade Commission's New Privacy Framework*, 67 FED. COMM. L.J. 293 (2015); M.T. Wroblewski, *Examples of Manipulative Advertising*, HOUS. CHRON. (Nov. 28 2018), http://smallbusiness.chron.com/examples-manipulative-advertising-11668.html; Kit Yarrow, *The Science of How Marketers (and Politicians) Manipulate Us*, TIME: MONEY (Sept. 29, 2016), http://time.com/money/4511709/marketing-politicians-manipulation-psychology/.

133 *See* Thomas R. Lee et al., *Trademarks, Consumer Psychology, and the Sophisticated Consumer*, 57 EMORY L.J. 575, 609 (2008).

media trade in their personal metrics. In the meantime, an industry whose valuation is well over three trillion dollars a year[134] goes largely unregulated.

Moreover, in a digital world, advertisers not only disseminate information to customers, they also gather data about them. The cookies that become embedded on computers after consumers visit certain websites can benefit those same consumers by speeding up retrieval of relevant and helpful information. However, they also allow companies to amass profiles of customers and ordinary visitors on their websites and then to retrieve them through JavaScript software.[135] The main beneficiaries of advertisement retrieval software are not audiences but advertisers, social media companies, the data mining firms, or political marketers.

One of the most effective internet campaigns of public misinformation occurred in 2016, when Russian intelligence services disseminated propaganda about Hillary Clinton, pilfered Democratic Party emails, and sent targeted audiences fake news stories meant to boost support for then–presidential candidate Donald Trump and presidential primary candidate Bernie Sanders. The U.S. intelligence services—specifically the FBI, CIA, and NSA—found that Russian intelligence services hacked a Democratic Party email server. WikiLeaks later very likely disseminated those documents, becoming, in the view of the FBI and CIA directors, either an advertent or inadvertent agent of the Russian Intelligence Services.[136]

Businesses like Cambridge Analytica (CA) specialize in harvesting digital profiles and using them to direct political advertisements to susceptible audiences. CA obtained data from subjects who voluntarily downloaded an app and provided private details, through misleading fronting that they were meant for an academic study. CA then accessed demographic information of eighty-seven million Facebook profiles to better tailor its messages and increase the effectiveness of its political marketing scheme.[137] Even if CA destroyed its datasets, there is reason to be concerned; Facebook indefinitely retains the originals to monetize at its discretion.[138]

---

134 *Market Capitalization of the Biggest Internet Companies Worldwide as of May 2018 (in Billion U.S. Dollars)*, STATISTA, https://www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/ (last visited Jan. 19, 2019).

135 Tsesis, *supra* note 122, at 437–38.

136 *See* Ellen Nakashima et al., *A German Hacker Offers a Rare Look Inside the Secretive World of Julian Assange and WikiLeaks*, WASH. POST (Jan. 17, 2018), https://www.washingtonpost.com/world/national-security/a-german-hacker-offers-a-rare-look-inside-the-secretive-world-of-julian-assange-and-wikileaks/2018/01/17/e6211180-f311-11e7-b390-a36dc3fa2842_story.html?utm_term=.8769cc6aa8e2; Kathryn Watson, *How Did WikiLeaks Become Associated with Russia?*, CBS NEWS (Nov. 15, 2017), https://www.cbsnews.com/news/how-did-wikileaks-become-associated-with-russia/.

137 *See* Craig Timberg et al., *Facebook: 'Malicious Actors' Used Its Tools to Discover Identities and Collect Data on a Massive Global Scale*, WASH. POST (Apr. 4, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/.

138 *See* Jane Wakefield, *Is Leaving Facebook the Only Way To Protect Your Data?*, BBC (Mar. 20, 2018), https://www.bbc.com/news/technology-43469656.

Under current U.S. law, Facebook may be liable for violating a 2011 consent decree for divulging eighty-seven million friendship profiles to the researcher who eventually shared them with CA.[139] As social media companies have grown wealthier by offering new products in exchange for personal information, they remain largely unaccountable for the enormous stores of information amassed on their servers. Any legislative attempt to limit social media companies will face Supreme Court doctrines that increasingly favor economic interests over the private concerns of individuals.[140] In the case of inflammatory statements made with actual malice, there is reason to rethink U.S. reliance on the marketplace of ideas to police itself. False political advertisements have been used to subvert the democratic process by saturating the marketplace of ideas with false propaganda that instigates violence, as it has in such countries as Sri Lanka, Indonesia, Libya, India, Myanmar, and Mexico.[141] The problem becomes increasingly acute as Facebook displaces local media, with news stories imputing the reputations of identifiable groups like Jews, African Americans, Muslims, and members of the LGBTQ community going viral on social media and being taken up by violent organizations seeking to harm the specters of their animus.

B. Judicial Review of False and Misleading Advertisements

The commercial speech doctrine assumes that advertisers will provide audiences with useful information. This in turn is thought to benefit the marketplace of ideas. But commercial speech does not always encourage thought and inspection. Rather, through repetition and exploitation of cognitive biases, which companies identify through algorithmic analyses, it elicits interests for brands through social imagery (call them "bells and whistles") rather than provides listeners with objective and informative truths about products.[142]

Typical consumer protection laws, which aim to prevent misrepresentation and material disclosures to protect audiences, are inadequate to deal

---

139 *See* Cecilia Kang, *Facebook Fine Could Total Billions if F.T.C. Talks Lead to a Deal*, N.Y. TIMES (Feb. 14, 2019), https://www.nytimes.com/2019/02/14/technology/facebook-ftc-settlement.html; Donie O'Sullivan, *Scientist at Center of Data Controversy Says Facebook Is Making Him a Scapegoat*, CNN (Mar. 20, 2018), https://money.cnn.com/2018/03/20/technology/aleksandr-kogan-interview/index.html.

140 *See* Amanda Shanor, *The New* Lochner, 2016 WIS. L. REV. 133.

141 *See* Alexander Tsesis, Essay, *Terrorist Speech on Social Media*, 70 VAND. L. REV. 651, 656 (2017); Libby Hogan & Michael Safi, *Revealed: Facebook Hate Speech Exploded in Myanmar During Rohingya Crisis*, GUARDIAN (Apr. 2, 2018), https://www.theguardian.com/world/2018/apr/03/revealed-facebook-hate-speech-exploded-in-myanmar-during-rohingya-crisis; Amanda Taub & Max Fisher, *Where Countries Are Tinderboxes and Facebook Is a Match*, N.Y. TIMES (Apr. 21, 2018), https://www.nytimes.com/2018/04/21/world/asia/facebook-sri-lanka-riots.html; Declan Walsh & Suliman Ali Zway, *A Facebook War: Libyans Battle on the Streets and on Screens*, N.Y. TIMES (Sept. 4, 2018), https://www.nytimes.com/2018/09/04/world/middleeast/libya-facebook.html.

142 *See* Doris Estelle Long, *Is Fame All There Is? Beating Global Monopolists at Their Own Marketing Game*, 40 GEO. WASH. INT'L L. REV. 123, 136 (2008).

with the digital platforms' uses of manipulative pricing discriminations informed by a wide range of past consumer behavior across various digital platforms.[143] While many data subjects find it convenient to receive targeted commercial advice and tailored political advertisements, algorithmic data processing often skews results, serving the interests of commercial and political entities, not the audiences' search for information.

Under these circumstances, courts should not rely on the heightened First Amendment scrutiny to review the regulation of misleading manipulative data acquired without explicit consumer consent, which at best has a minimum value to consumers. Indeed, much of it is not advertisement delivery but data acquisition and sale. Social media companies are subject to ordinary commercial regulation, with no intermediate scrutiny requirement, when they falsely claim to solely be platforms for information but actually exploit their market strength to trade in limitless private data. Social media companies based in the United States—such as Google, Facebook, and Twitter—can be limited in the for-profit aspects of their business. Intermediate scrutiny applies to their advertisements. But exchange in private data should be governed by reasonable commercial regulation.[144] Regulation of the internet communication is subject to heightened scrutiny because it involves speech. But regulations of it should be subject to intermediate scrutiny because the World Wide Web is neither a purely commercial nor a purely speech platform. Part IV of this Article will argue that reasonable time, place, and manner restrictions can be made on the duration of data retention.

The Court has been clear that misleading commercial speech is not protected by the First Amendment.[145] Regulations that control only misleading commercial statements should receive rational basis scrutiny. In this category are laws governing lending, where internet service companies track, rather than inform, customers using online behavioral advertising.[146] The Federal Trade Commission Act (FTCA) specifically prohibits "unfair or deceptive acts or practices."[147] Just as the Federal Trade Commission (FTC) has found that the unintentional release of consumer names and email addresses linked to medical care can be unfair and deceptive,[148] so too should the purposeful failure to inform consumers of the extent social media companies share consumers' private information with third-party vendors. Three-quarters of

143 *See* Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 190 (2017).

144 *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 596 (2011) (Breyer, J., dissenting) ("The fact that the Court normally exempts the regulation of 'misleading' and 'deceptive' information even from the rigors of its 'intermediate' commercial speech scrutiny testifies to the importance of securing 'unbiased information.'").

145 Nat'l Inst. of Family & Life Advocates v. Becerra, 138 S. Ct. 2361, 2382 (2018); *In re* R.M.J., 455 U.S. 191, 203 (1982).

146 *See* Alan L. Friel, *Managing Risk from Advertising and Sales Promotions*, INTELL. PROP. & TECH. L.J., Feb. 2012, at 3, 5–6.

147 15 U.S.C. § 45(a)(1) (2012).

148 Eli Lilly & Co., 133 F.T.C. 763 (2002) (consent order).

Americans, as a study relying on data from 543 subjects found, do not even read privacy statements.[149] The Global Privacy Enforcement Network, a multinational information privacy task force, found that about a fourth of privacy statements lacked adequate indication of what personal data was been collected; sixty-five percent lacked a statement about what protections were used to maintain privacy; and about seventy percent of policy statements failed to indicate what country data would be stored in, making it impossible for users to know what law(s) would apply.[150] In the United States, a national law should be passed that "[a]llow[s] consumers the right to request a business to disclose the categories and specific pieces of personal information that the business has collected about the consumers as well as the source of that information and business purpose for collecting the information."[151]

In identifying factors that mislead consumers, courts can look to the FTC's fair information practices, which require adequate "[n]otice, [c]hoice, [a]ccess, and [s]ecurity."[152] But the judiciary's role is of greater consequence than that of the FTC, which only prosecutes cases of companies failing to live up to their own privacy statements.[153] Judges should look to whether privacy statements allowing for blanket use of private data are so ambiguous as to result in consumer confusion capitalized up by firms to sell intimate information to which data subjects did not directly consent.

Political data, however, is different. With that type of communication, even false information can have some value to vigorous discussion on public issues.[154] First Amendment jurisprudence recognizes the importance to representative government of being free to criticize or support political positions. *New York Times Co. v. Sullivan* identified a standard for regulating defamatory speech about how public servants carry out their official

149 Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, INFO., COMMC'N & SOC'Y, July 2018, at 1, 8.

150 *Privacy Statement Deficiencies Could Have Greater Consequences in 2018*, MAYNARD COOPER & GALE, https://www.maynardcooper.com/blog/privacy-statement-deficiencies-could-have-greater-consequences-2018 (last visited Jan. 23, 2019).

151 *State Laws Related to Internet Privacy*, NAT'L CONF. ST. LEGISLATURES (Jan. 7, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx (citing CAL. CIV. CODE §§ 1798.100–.198); *see also* CAL. CIV. CODE §§ 1798.83–.84 (West 2018); UTAH CODE ANN. §§ 13-37-201–03 (West 2018).

152 FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS, at i (2000) [hereinafter FTC PRIVACY ONLINE REPORT], https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf .

153 *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 599, 628–29 (2014).

154 *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 271–72 (1964) (stating that First Amendment values do not only apply to true statements and adding "[t]hat erroneous statement is inevitable in free debate, and that it must be protected if the freedoms of expression are to have the 'breathing space' that they 'need . . . to survive'" (quoting NAACP v. Button, 371 U.S. 415, 433 (1963)).

duties.[155] That case arose from a lawsuit filed by the supervisor of the Montgomery, Alabama, police department, whom a civil rights organization criticized for refusing to comply with desegregation orders.[156] The advertisement critical of the department's treatment of a civil rights matter contained a number of mistakes.[157]

Supervisor Sullivan was neither mentioned in the advertisement, nor could he show evidence of suffering harm.[158] Nevertheless, the jury returned a verdict awarding him a half million dollars in damages. The Supreme Court overturned that verdict and established a far-reaching rule. It held that a public official bringing a lawsuit for damages incurred from a statement about the performance of official duties show with convincing clarity that the speaker acted with knowledge or with reckless disregard of the statement's falsity.[159] The *Sullivan* Court recognized that defamation can provide relief from false statements that harm an individual's reputation.[160] Yet it overturned the jury verdict because of a higher principle at play.

Public debate on and off the internet is so essential to deliberative democracy that even erroneous statements harming a public servant's reputation must be tolerated absent actual malice.[161] Moreover, even outside the defamation context, discussing controversial subjects inevitably causes discomfort and even emotional pain, but these are not reasons for silencing individuals on the internet. Political conflicts tend to be heated and given to hyperbole or understatement, some of them demonstrably false. The importance of open and frank discussions is of such high consequence to the proper functioning of representative politics that "occasional injury to the

---

155 *Id.*

156 *Id.* at 256–57. To view the advertisement see *Heed Their Rising Voices*, N.Y. TIMES, Mar. 29, 1960, at L25.

157 *Sullivan*, 376 U.S. at 258 ("It is uncontroverted that some of the statements contained in the two paragraphs were not accurate descriptions of events which occurred in Montgomery."); *id.* at 258–59 (listing discrepancies between the ad and events of desegregation protests).

158 *Id.* at 294 (Black, J., concurring).

159 *Id.* at 279–80 (majority opinion) ("The constitutional guarantees require, we think, a federal rule that prohibits a public official from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with 'actual malice'—that is, with knowledge that it was false or with reckless disregard of whether it was false or not."); *id.* at 285–86 ("[W]e consider that the proof presented to show actual malice lacks the convincing clarity which the constitutional standard demands.").

160 *Id.* at 267 (stating that the defendant's "privilege of 'fair comment' for expressions of opinion depends on the truth of the facts upon which the comment is based").

161 *See* Caldwell v. Caldwell, 545 F.3d 1126, 1133 (9th Cir. 2008) ("An interest in informed participation in public discourse is one we hold in common as citizens in a democracy."); Detroit Free Press v. Ashcroft, 303 F.3d 681, 711 (6th Cir. 2002) ("A true democracy is one that operates on faith—faith that government officials are forthcoming and honest, and faith that informed citizens will arrive at logical conclusions.").

reputations of individuals must yield to the public welfare."[162] This mode of reasoning and the rule from *Sullivan* has some troubling implications for politics. Under current doctrine, the Court is likely to strike down any legislation seeking to regulate purely political speech, especially if it limits communication about public officials and public matters.[163] And it is worth putting such protections of speech but not shirking from regulating actually malicious falsehoods that deceive the electorate as they did during the 2016 presidential election. That is, even in compelling speech matters there are countervailing considerations, such as fair elections that can advance compelling government reasons and are narrowly tailored.

However, where incitement or true threats are called for, the actual malice test is inapplicable, nor is that expression covered by the First Amendment. Under the latter circumstances, either the *Brandenburg v. Ohio* test,[164] with its imminent threat of harm component, or the *Virginia v. Black* true threats test applies.[165]

The Court is unlikely to revisit the issues anytime soon despite the profound effect false political speech had on the 2016 election. Political speech, even when misleading but not actually malicious, remains protected by the First Amendment when dealing with public matters and public concerns. Public debates about federal and state matters require freedom from government intrusions. Free speech principles prevent the stifling of open debate about democratic institutions and actors. The internet is a network for the free exchange of ideas. Working out complex social, cultural, and political issues is a step to finding the truth about how to make legal changes needed that better serve the general welfare. Yet, when internet firms receive notices complaining of deliberate falsehoods, they should investigate with the help of natural humans, capable of making nuanced semantic and syntactic evaluations.

U.S. free speech law amply protects the marketplace of digital ideas. Nevertheless, while voting rights are fundamental, states can regulate them through fair and efficient legislation designed to maintain the integrity of elections.[166] Federal action is warranted and legitimate where social media and other internet intermediaries have been notified that they are carrying misleading information about elections, and fail to investigate and take it down. Hence, posts can be regulated and enjoined when they mislead voters of the date of the election, falsely identify locations of voting booths, misstate

162 *Sullivan*, 376 U.S. at 281 (quoting Coleman v. MacLennan, 98 P. 281, 286 (Kan. 1908)).

163 The Court has found corporations have First Amendment rights. *See* First Nat'l Bank of Bos. v. Bellotti, 435 U.S. 765, 784–85 (1978).

164 Brandenburg v. Ohio, 395 U.S. 444, 447 (1969).

165 Virginia v. Black, 538 U.S. 343, 359, 364–65 (2003).

166 *See* Burdick v. Takushi, 504 U.S. 428, 433 (1992) ("[T]o subject every voting regulation to strict scrutiny and to require that the regulation be narrowly tailored to advance a compelling state interest, as petitioner suggests, would tie the hands of States seeking to assure that elections are operated equitably and efficiently.").

candidates' official affiliation, or falsify information about the order on the official ballot, and so forth. As discussed in Part IV, changes should be made to the current state in internet firm immunity to hold them accountable for being complicit in knowingly misleading the public about commercial or political information.

IV. Regulating Retention of Data

Democratic societies function best in a market where divergent political and personal opinions can thrive. The spread of divisive information can, on the other hand, divide citizens by racist, sexist, and xenophobic rhetoric that shifts the marketplace of ideas away from rational, scientific, and artistic expression.[167] Unlike government, commercial outlets need not operate for the general welfare. Profit-driven internet businesses are important to the economy, but a for-profit corporation need not spend resources to address political problems or advance equal opportunity. Indeed, at times commercial institutions sow false discourse, as when corporations seek to deceive about health risks and climate change in order to advance commercial tobacco and energy interests.[168] With advertisements, government has an important interest in enforcing carefully crafted laws requiring accurate commercial information.[169] Algorithmic models help marketers profit and customers gain valuable knowledge about matters such as price and store location. However, commercial information does little to advance democratic deliberation, personal autonomy, or objective knowledge.[170]

As matters stand in the United States, social media companies are immune from liability even when they knowingly host false or misleading advertisements on their platform to which they did not contribute. Congress should modify the immunity statute, section 230, which is discussed in Section IV.B, to put regulatory responsibility on multibillion-dollar corporations to better police their networks against false and misleading advertisements or to face large monetary penalties.

A. False and Misleading Digital Messages

Internet firms develop, modify, and improve algorithms in order to improve their products. A corporation's obligation is to increase profits for its stockholders.[171] Thus, optimizing search and website content is for the

167 *See* Paul Przybylski, Note, *A Common Tool for Individual Solutions: Why Countries Should Establish an International Organization to Regulate Internet Content*, 9 VAND. J. ENT. & TECH. L. 927, 936 (2007).

168 *See generally* NAOMI ORESKES & ERIK M. CONWAY, MERCHANTS OF DOUBT: HOW A HANDFUL OF SCIENTISTS OBSCURED THE TRUTH ON ISSUES FROM TOBACCO SMOKE TO GLOBAL WARMING (2011).

169 *See supra* notes 157–59 and accompanying text.

170 For a detailed study about the various constitutional theories of free speech, see Tsesis, *supra* note 27.

171 *See* Dodge v. Ford Motor Co., 170 N.W. 668, 684 (Mich. 1919).

advancement of capitalistic motives, rather than the truth.[172] Information thereby analyzed and generated through artificial intelligence tools enables firms to tailor and target product information to receptive audiences. Insofar as the information is in the interest of consumers, the data serves the marketplace of ideas. Digital algorithmic learning has proven to be highly profitable. In addition to commercial products, such algorithmic systems have helped countless people find all manner of curiosities and news online that stimulate self-expression or political discourse. But to the extent that algorithms skew and manipulate digital traffic, their value for advancing truth is low.[173]

There are also abundant risks with an unregulated marketplace populated with firms seeking to cash in by using consumer profiles to manipulate their political behaviors. The rate of digital advancement poses one of the greatest hurdles for policymakers seeking to control the spread of "fake news." Norms protecting consumers already exist, but they are underenforced. The Federal Trade Commission has long accepted Fair Information Practice Principles (FIPP), which require data collectors to provide consumers with "clear and conspicuous notice of their information practices, including what information they collect, [and] how they collect it."[174] That standard has proved inadequate, however, because firms' disclosures are typically so broad and vague that they provide audiences inadequate control over the information they divulge to social media corporations in exchange for digital services. The lack of transparency arguably violates the FIPP's guidance to clearly identify "any potential recipients of the data."[175] Consumers are usually left in a black box of unknowability of whom their data is being harvested to and how long it is being stored. Greater regulatory oversight is needed to protect users' privacy and control over data. Facebook, for instance, should not have been left immune from liability for the havoc, fraud, and privacy breaches it facilitated during the 2016 U.S. presidential election.[176] It became a platform for misleading information, profiting from

172 AMY N. LANGVILLE & CARL D. MEYER, GOOGLE'S PAGERANK AND BEYOND 28 (2006).

173 Elizabeth E. Joh, *Private Security Robots, Artificial Intelligence, and Deadly Force*, 51 U.C. DAVIS L. REV. 569, 583–84 (2017).

174 FTC PRIVACY ONLINE REPORT, *supra* note 152; *Fair Information Practice Principles*, FED. TRADE COMM'N, https://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last modified June 25, 2007). The "five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress." *Id.*

175 *Id.*

176 Facebook also has data partnerships for personal data being shared with companies like Apple, Samsung, and Amazon. Nicholas Confessore et al., *Facebook Back on the Defensive, Now Over Data Deals with Device Makers*, N.Y. TIMES (June 4, 2018), https://www.nytimes.com/2018/06/04/technology/facebook-device-partnerships-criticized.html. Moreover, Facebook has shared information with Chinese companies, including one (Huawei) with close relations to the Chinese autocracy. Michael LaForgia & Gabriel J.X. Dance, *Facebook Gave Data Access to Chinese Firm Flagged by U.S. Intelligence*, N.Y. TIMES (June 5, 2018), https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html.

deception, aware but not informing customers whose information had been divulged to Cambridge Analytica.[177] Later in this Article, I will explain changes to U.S. law that could have made such prosecution possible.

Ideally, consumer policy should cover a breadth of intrusive online behaviors through self-help civil actions and government prosecutions. To systematically deal with internet firms' continuous and clandestine gathering of private metrics, a legal threshold should be established delimiting the duration that a marketer can retain personalized data. The monitoring technologies are meant to shape human behavior, not as steps to social truths or personal revelations, but for profit. As commercial speech, intermediate scrutiny should enable courts to balance the interests of government and private party, protect the due process sufficient for fair adjudication, and provide a mechanism for redress, such as a contextually sound injunction of the case or controversy. Where restrictions are made on commercial vendors disseminating false political speech or journalism, better known as "fake news," an actual malice standard should apply to better protect controversial public statements.

Given internet companies' substantial effects on interstate economy, Congress can rely on Commerce Clause authority to penalize firms that use their market power to manipulate searches that, in the end, prevent consumers from viewing the full breadth of useful information.[178] The manipulation of search engine results, for instance, tends to produce more consumerist speech that favors dominant commercial speakers who seek to sell their products rather than provide objective, truthful information to consumers.[179] Moreover, regulation should be used to limit the length of time for which a merchant can retain data and prohibit the resale of data to third-party businesses not engaged in enterprises directly related to the original service. The idea is to maintain consent and control in the hands of consumers, rather than those of data marketers.

Currently, internet information providers are for the most part shielded from liability by the Communication Decency Act's safe harbor provision.[180] Facebook, Google, Twitter, and YouTube can shield themselves behind the law from liability for false material, exploitative content, misinformation,

177 Anthony Cuthbertson, *Facebook Knew About Cambridge Analytica Data Breach a Year Before Trump Election*, INDEPENDENT (Apr. 6, 2018), https://www.independent.co.uk/news/business/news/facebook-cambridge-analytica-trump-election-data-breach-mark-zuckerberg-a8292071.html.

178 ALBERT-LÁSZLÓ BARABÁSI, LINKED: HOW EVERYTHING IS CONNECTED TO EVERYTHING ELSE AND WHAT IT MEANS FOR BUSINESS, SCIENCE, AND EVERYDAY LIFE 44 (2002) (finding a "*complete* absence of democracy, fairness, and egalitarian values on the Web" that "prevents us from seeing anything but a mere handful of the billion documents out there").

179 *See* Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149, 1165–67 (2008).

180 47 U.S.C. § 230(c)(1) (2012).

propaganda, and malicious fake news.[181] Advertisements do not always benefit consumers. Advertisers principally sell products, not engage in what has traditionally been thought to be the marketplace of ideas.

The Supreme Court has recognized that false and deceitful advertisement does not fall within the ambit of First Amendment protections. Digital misinformation about politics and products is unprotected by the commercial speech doctrine. In *Central Hudson*, the Court found the Free Speech Clause protects those advertisements that inform the public, but not those that are false and misleading.[182]

Even when websites provide visitor numbers, with which they seek to demonstrate popularity, their definitions are problematic. About fifty-two percent of internet traffic is generated by bots, not natural people.[183] Tim Wu explains that "bots pose as humans on Facebook, Twitter, and other social media, and they transmit messages as directed" including hundreds of millions of governmental and private-actor posts.[184] Their influence on internet traffic should not be understated with the extent to which private parties and governments use them to spread false information and propaganda,[185] which diminishes the value of the internet to the marketplace of ideas. Some bots disseminate foreign propaganda to which only rational basis scrutiny applies because of the national defense concerns they invoke.[186] On the commercial side, there are social benefits of truthful information and harms from misleading and manipulative speech. In neither case are they part of the marketplace for truth as it has been defined in First Amendment jurisprudence. Bot messaging is rather a technical tool for

181 *See* Julia Carrie Wong, *Former Facebook Executive: Social Media Is Ripping Society Apart*, GUARDIAN (Dec. 12, 2017), https://www.theguardian.com/technology/2017/dec/11/facebook-former-executive-ripping-society-apart.

182 Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 563–64 (1980).

183 Adrienne LaFrance, *The Internet Is Mostly Bots*, ATLANTIC (Jan. 31, 2017), https://www.theatlantic.com/technology/archive/2017/01/bots-bots-bots/515043/.

184 Tim Wu, *Is the First Amendment Obsolete?*, KNIGHT FIRST AMEND. INST. (Sept. 2017), https://knightcolumbia.org/content/tim-wu-first-amendment-obsolete.

185 *See* Alex Hern, *Facebook and Twitter Are Being Used to Manipulate Public Opinion—Report*, GUARDIAN (June 19, 2017), https://www.theguardian.com/technology/2017/jun/19/social-media-proganda-manipulating-public-opinion-bots-accounts-facebook-twitter; Timothy Tam, *How Bots Are Manipulating Cryptocurrency Prices*, VENTUREBEAT (Dec. 14, 2017), https://venturebeat.com/2017/12/14/how-bots-are-manipulating-cryptocurrency-prices/.

186 DANIEL FRIED & ALINA POLYAKOVA, ATL. COUNCIL, DEMOCRATIC DEFENSE AGAINST INFORMATION 4 (2018), https://disinfoportal.org/wp-content/uploads/ReportPDF/Democratic-Defense-Against-Disinformation.pdf ("Russian manipulation of social media utilizes unattributed political ads or officially organized bots, trolls, cyborgs (human/bot combinations), and other means of mounting and masking disinformation campaigns."); Robert Gorwa, *Computational Propaganda in Russia: The Origins of Digital Misinformation*, OXFORD INTERNET INST., https://www.oii.ox.ac.uk/blog/computational-propaganda-in-russia-the-origins-of-digital-misinformation/ (discussing Russian propaganda methods, including the use of bots, to manipulate social media information by exploiting internet architecture).

exaggerating, generating such an overwhelming amount of false information to silence countervoices, and thereby confusing the public. Robotic messaging can be used to attack deliberative democracy's administrative tools. "[U]nder the existing jurisprudence, it seems that little—other than political norms that are fast eroding—stands in the way of a full-blown campaign designed to manipulate the political speech environment to the advantage of current officeholders."[187] An Association of National Advertisers' report found: "Sophisticated bots moved the mouse, making sure to move the cursor over ads. Bots put items in shopping carts and visited many sites to generate histories and cookies to appear more demographically appealing to advertisers and publishers."[188] Social media websites drive up advertisement costs by reporting earnings based on inflated reports about internet traffic.[189]

In addition to their commercial use, bots spread political messages. Some of those posts are racially charged, as during the 2016 presidential election or the 2017 Virginia gubernatorial race, to impact elections and product sales.[190] Many target data profiles based on algorithmically identified biases and vulnerabilities. Messages target individuals who are most often unaware they have been profiled.[191] Analytics companies, such as Cambridge Analytica, earn enormous revenues by using psychometrics to understand commercial and civic behaviors. They then compose and transmit emotive and manipulative commercials in order to alter people's beliefs and behaviors.[192] As one author disturbingly put it: "[C]an you imagine what Hitler would have done with access to Facebook data on tens of millions of people?"[193]

---

187 Wu, *supra* note 184.

188 WHITE OPS, INC. & ASS'N OF NAT'L ADVERTISERS, THE BOT BASELINE: FRAUD IN DIGITAL ADVERTISING 6 (2014), https://www.whiteops.com/hubfs/ANA_WO_Bot_Baseline_2014-1.pdf?t=1505782715097.

189 *See* Michael Burgi, *What's Being Done to Rein in $7 Billion in Ad Fraud*, ADWEEK (Feb. 21, 2016), https://www.adweek.com/brand-marketing/whats-being-done-rein-7-billion-ad-fraud-169743/.

190 *See* Kevin Robillard, *Bots Stoke Racial Strife in Virginia Governor's Race*, POLITICO (Nov. 3, 2017), https://www.politico.com/story/2017/11/03/virginia-governors-race-bots-racial-strife-244534.

191 *See* Gabriel Gatehouse, *Did Cambridge Analytica Play a Role in the EU Referendum?*, BBC NEWSNIGHT (June 27, 2017), https://www.bbc.com/news/av/uk-40423629/did-cambridge-analytica-play-a-role-in-the-eu-referendum.

192 *See* Justin Bariso, *Facebook, Cambridge Analytica, and the Dark Side of Emotional Intelligence*, INC. (Mar. 26, 2018), https://www.inc.com/justin-bariso/facebook-cambridge-analytica-dark-side-emotional-intelligence.html ("Among other things, Cambridge Analytica aimed to help clients identify the emotional triggers of voters, so they could motivate those voters to act."). As a spokesman for Virginia's Democratic Senator Mark Warner put it: "What we saw during the 2016 presidential campaign was a consistent and coordinated effort by trolls and bots to 'flood the zone' to manipulate the conversation on social media." Robillard, *supra* note 190.

193 Bariso, *supra* note 192.

Those who harvest the most data are multibillion-dollar social media conglomerations. This is especially a concern with the spread of at-home voice recognition devices, like Amazon's Echo/Alexa commercial device, and the growing presence of the Internet of Things. Further, Google and its popular YouTube service are not simply informative. They earn a percentage from each click on an advertisement, irrespective of who accesses it.[194] Facebook likewise earns revenues for each click on an advertisement.[195] Facebook "likes" can be bought to harvest feed hits, and Twitter followers can also be obtained for a price.[196] Social media architecture is designed to benefit advertising, not strictly the marketing of commercially or politically beneficial data. By facilitating the dissemination of false advertisement and generating inaccurate data, social media companies are often conduits to frauds.

Despite the extent of deceptions, misinformation, and manipulation being perpetrated over internet information providers' websites, a provision of the Communications Decency Act (CDA) prevents federal regulators or private parties from filing suits against them. In relevant part, section 230 of the CDA grants immunity to "provider[s] or user[s] of an interactive computer service" from liability for third-party content on the platforms.[197] Judges have held platforms are immune even when they had notice that defamatory content appeared on their websites but, nevertheless, refused to eliminate it.[198]

B. Section 230 Immunity

Section 230 applies to internet service providers who host third-party content. The statute provides: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[199] This has not only achieved the stimulation of robust debates and artistic platforms—which for good reason courts, legislators, and scholars favor[200]—but also the diminution of privacy. Under this current regime, internet service providers are expected to police their own sites for offensive content, to self-regulate the

194 *See* Robert Cookson, *Brands Versus Bots*, FIN. TIMES (July 19, 2016), https://www.ft.com/content/fb66c818-49a4-11e6-b387-64ab0a67014c; Eric Rosenberg, *How Google Makes Money (GOOG)*, INVESTOPEDIA (Dec. 5, 2018), https://www.investopedia.com/articles/investing/020515/business-google.asp.

195 *See How Does Facebook Make Its Money?*, BUS. MGMT. DEGREES, https://www.business-management-degree.net/facebook/ (last visited Feb. 1, 2019).

196 *See* Doug Bock Clark, *The Bot Bubble*, NEW REPUBLIC (Apr. 20, 2015), https://perma.cc/M33U-H5K2.

197 47 U.S.C. § 230(c)(1) (2012).

198 *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 331–34 (4th Cir. 1997).

199 47 U.S.C. § 230(c)(1).

200 *See, e.g.*, Barrett v. Rosenthal, 146 P.3d 510, 525 (Cal. 2006); Nicholas W. Bramble, *Safe Harbors and the National Information Infrastructure*, 64 HASTINGS L.J. 325, 358 (2013); Joseph Monaghan, Comment, *Social Networking Websites' Liability for User Illegality*, 21 SETON HALL J. SPORTS & ENT. L. 499, 506 (2011).

dissemination of personal data, to market user profiles, to target vulnerable persons, to manipulate personality profiles, and to effectively remove it. By passing the safe harbor provision, Congress aimed to protect internet information providers against litigation for simply screening, removing, or blocking materials that they in good faith believe to be "excessively violent . . . or otherwise objectionable."[201] Social media companies have relied on this policy to avoid liability, even when their services encouraged illegal conduct.[202] Only when a website materially contributes to illegal content does it lose its immunity,[203] allowing it to host unedited third-party posts with virtual impunity.

Circuit courts have deferred to Congress's reliance on corporate self-policing to uphold section 230 immunity.[204] The approach overly relies on internet companies to put in good faith efforts to monitor the marketplace of ideas for illegality. The expectation is that firms will independently remove false and misleading advertisements. Even if those companies could be trusted to act effectively and consistently on that mission, it does not, at all, get to the problem of countless privacy infringements so common in the digital realm. Companies enjoy immunity for harvesting audience profiles through the use of digital technologies such as cookies, deep packet searches, facial recognition technology, IP address selection, and internet service protocols. These only have a tangential connection to spreading truth in the marketplace of ideas. They primarily profit companies, who then make corporate decisions, some of which deeply harm natural people's privacy.

Of late, scholars have questioned whether social media services are merely distributors of content rather than information providers.[205] Under the current system, as Professor Danielle Citron and Benjamin Wittes have pointed out, courts have granted immunity to a variety of internet platforms even when those platforms intend to disseminate abuse and provide electronic forums for illegal conduct.[206] They propose revision of section 230 to subject those platforms to liability for the harms of defamation, revenge

---

201 47 U.S.C. § 230(c)(2)(A); *see also Zeran*, 129 F.3d at 331 ("Congress enacted § 230 to remove the disincentives to selfregulation . . . .").

202 *See, e.g.*, Jones v. Dirty World Entm't Recordings LLC, 755 F.3d 398, 401–03 (6th Cir. 2014).

203 *See, e.g.*, Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1167–70 (9th Cir. 2008).

204 *See* Batzel v. Smith, 333 F.3d 1018, 1020 (9th Cir. 2003); Green v. Am. Online, 318 F.3d 465, 470 (3d Cir. 2003); Ben Ezra, Weinstein, & Co. v. Am. Online Inc., 206 F.3d 980, 986 (10th Cir. 2000).

205 *See* Susan Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 HARV. J.L. & TECH. 569, 637–42 (2001); Sewali K. Patel, Note, *Immunizing Internet Service Providers from Third-Party Internet Defamation Claims: How Far Should Courts Go?*, 55 VAND. L. REV. 647, 651–53 (2002).

206 Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 408 (2017).

porn, and other violations of trust that have no place in the marketplace of ideas.[207]

Given the severity of privacy intrusion, lawmakers should modify section 230 to require internet companies to more effectively monitor their sites for manipulatively false advertisements. Offenders should be subjected to prosecution. That includes monitoring foreign state entities who employ propaganda advertising on U.S. social media sites to influence American elections.

C. Limiting Storage of Digital Data

Moreover, upon request, internet information providers should be required to delete data from corporate servers once it is no longer needed to advance the function for which they were originally posted.[208] This policy should hold for commercial advertisements and political psychometrics aggregated by internet intermediaries. What is more, as with other news outlets social media companies should provide the FCC and consumers complete reports of how they market and use private information about persons who use their websites or others connected to them. Privacy policy should be governed by regulatory oversight, not corporate initiatives. A modified Communication Decency Act or, in the alternative, a new federal statute should allow the Justice Department and private consumers to file civil lawsuits against internet offenders, maintaining a rational basis test for misleading and false commercial advertisements.

Under current U.S. laws, data mining is lawful, but without consumer control over their digital profiles, intimate details can be resold indefinitely without clear consent to those commercial transactions. The corporate agglomeration of commercial digital data should be dealt with at the congressional level because it requires collective action policy.[209] Internet services entice users to divulge private information by offering them helpful, entertaining, political, and generally fascinating services. There is little consent where the information digital companies provide is misleading about resale to third parties and about permanent retention.

A model already exists that can provide guidance to U.S. lawmakers. The Charter of Fundamental Rights of the European Union establishes a standard that limits internet information companies' retention and processing of data for the "specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[210] The European Data Protection Directive of 1995 then obligated EU member states to prohibit dissemination of personal data unless they first obtain the

---

207 *Id.* at 417–18.

208 This would be in keeping with EU law, which limits the duration for which social media providers can retain personal information to the period needed to advance "specified, explicit and legitimate purposes." Directive 95/46/EC, *supra* note 77, at 31, 40.

209 *See* NFIB v. Sebelius, 567 U.S. 519, 595 (2012) (Ginsburg, J., dissenting) ("Congress' intervention was needed to overcome this collective-action impasse.").

210 Charter of Fundamental Rights of the European Union, art. 8, 2012 O.J. (C 326) 391.

unambiguous consent for specific data processing, required to fulfill a contractual obligation, to abide by a legal duty, to protect the data subject's vital interests, or to perform a public function by an authorized official.[211]

The 1995 Directive was superseded by the EU General Data Protection Regulation ("GDPR") that now controls corporate use of digital data.[212] Many facets of the older law remain. Under the GDPR, companies can only control personal data for "specified, explicit and legitimate purposes."[213] There is a limit for how long data subjects' information can be saved on servers. This significantly limits internet companies' abilities to commodify ordinary people's private details. Another GDPR provision protects listeners against corporate internet firms' resale of data to third parties: "Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation."[214] Therefore, the length of time for which data can be retained does not apply to parties engaged in the stated activities.

The GDPR is a law subject to EU free speech norms, which are not the same as those in the United States. The U.S. Supreme Court tends to be more protective of free speech than its European counterparts. But the GDPR provides U.S. lawmakers with a framework for how long internet intermediaries can retain information. Any new U.S. law must be in keeping with Supreme Court commercial speech precedents. One important distinction is that instead of the European reasonableness test,[215] American courts should apply the intermediate scrutiny test to regulate commercial transactions between internet information intermediaries and consumers who expose their personal data to the vendor. Congress has a substantial interest in protecting consumers against the exploitation of their data without explicit data subjects' consent. Such a U.S. law should be narrowly tailored to meet carefully crafted government policy that would enable commercial entities to disseminate information and consumers to guard their private data from permanent commercial exploitation.

D. Fake News and Disinformation

In an age of such immense private data retention, the U.S. should join Europe by adding consumer privacy regulations of the internet to better preserve natural persons' fundamental rights to dignity, autonomy, and privacy.[216] In January 2018, the European Commission (EC) convened a high-level group of experts to address the growing phenomenon of "fake news and

211 Directive 95/46/EC, *supra* note 77, at 46.

212 GDPR, *supra* note 4, at 1, 35, art. 5(b).

213 *Id.*

214 *Id.* at 28, recital 153.

215 Directive 95/46/EC, *supra* note 77, at 40.

216 *Id.* at 38, art. 1 ("In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.").

disinformation spread online."[217] The definition for fake news is very precise. The category does not include defamation, hate speech, or incitement to violence. Rather, the EC enjoined the experts to concentrate on how to combat "misleading information designed, presented and promoted to intentionally cause public harm or for profit."[218] Or, put into U.S. terms, the EC addressed speech detrimental to the marketplace of ideas.

A group of experts created a report advising the EC to avoid censorship. They proposed a dynamic process of identifying and addressing risks and harms. The experts recommended a multifactoral analytical construct of interconnected factors.[219] They included a call for increased transparency, promotion of literacy about media and information, user and journalist empowerment "to tackle disinformation and foster a positive engagement with fast-evolving information technologies," maintaining multiplicity of news sources, and engaging in future research.[220] This thoughtful approach offers a path toward dialogue conducive to consumers' acquisition of useful, artistic, philosophical, and political messages. In the meantime, issues such as compromises of private computer servers, such as the 2016 presidential campaign break-in and re-publication of the Democratic Party's emails, will need to be tackled more directly. Establishing think tanks with indefinite time lines will help move the ball forward in the future, but the extent of privacy breaches also requires immediate action. The threat of foreign interference in elections, for instance, is an immediate threat to democracy and remote from the marketplace of ideas.

But the U.S. libertarian tradition to free speech makes moving U.S. law in the direction of European balancing idealistic, rather than anything likely to occur in the near future. In the short term, Congress should pass a law pursuant to its Commerce Clause authority that will limit the length of time for which internet firms can retain data, require firms to use an opt-in option, and also modify section 230 of the Communications Decency Act to remove immunity of merchants who save data without consent of users; who disseminate it to third parties without consent of the data subject; who knowingly direct false and malicious information on their servers; and who maintain a data brokerage system without the express, transparent, and informed consent of the data subjects.

CONCLUSION

Consumers benefit from truthful advertisements; however, digital platforms do not merely inform consumers. They are also harvesting intimate

217 EUROPEAN COMM'N, A MULTI-DIMENSIONAL APPROACH TO DISINFORMATION: REPORT OF THE INDEPENDENT HIGH LEVEL GROUP ON FAKE NEWS AND ONLINE DISINFORMATION 5 (2018), https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

218 *Id.* at 10.

219 For a discussion of multifactoral speech analysis, see Alexander Tsesis, *Multifactoral Free Speech*, 110 NW. U. L. REV. 1017 (2016).

220 EUROPEAN COMM'N, *supra* note 217, at 5.

details about their customers. What is more, the false advertisements available through platforms such as Google, Facebook, and Twitter threaten to emotively manipulate consumer behavior. Distortion extends to the political realm with manipulative search results and bot posts that threaten deliberative democracy. Facebook's recent announcement that it will require political advertisers to reveal their identities will not be nearly enough to resolve the problem.[221] As the Supreme Court observed in *Turner Broadcasting System, Inc. v. FCC*, the First Amendment "does not disable the government from taking steps to ensure that private interests not restrict, through physical control of a critical pathway of communication, the free flow of information and ideas."[222]

Social media companies should not be self-regulated but should also not be regulated under the framework of commercial regulations of digital platforms. Otherwise, digital platforms continue indefinitely retaining data subjects' personal information long after completion of commercial transactions. Digitally stored materials, then, not only remain available for third-party transactions but also, unbeknownst to data subjects, susceptible to third-party exploitation for purposes unrelated to the original transaction. The Cambridge Analytica debacle appears to have been just that sort of snafu in Facebook's corporate plan, which cost at least eighty-seven million people their privacy and manipulated the 2016 U.S. presidential race.[223]

Enforcing standards against fake commercial and political advertisements, whether under the guise of news reporting or for commercial products, is an important governmental interest that can be applied in a narrowly tailored manner to benefit audiences, without stifling meaningful debate. It should start with a statutory requirement that social media companies use opt-in rather than opt-out requirements for divulging private users' data. Social media platforms that facilitate the dissemination of private information or false advertisements should be unable to hide behind the mantle of section 230's safe harbor provision. Without litigation, including discovery proceedings, only social media programmers can identify whether the information intermediaries are aware that they are being enriched through false advertisements.

Commerce Clause authority enables Congress to limit the duration for which marketers can retain consumer data and limit the purposes for which

221 Tony Romm, *Facebook's New Rules Aim to Thwart the Kind of Ads Bought by Russian Trolls During the Election*, WASH. POST (Apr. 6, 2018), https://www.washingtonpost.com/news/technology/wp/2018/04/06/facebooks-new-rules-aim-to-thwart-the-kind-of-ads-bought-by-russian-trolls-during-the-election (reporting that "Facebook will then require entities that seek to purchase issues-based ads to first verify who they are and their location offline").

222 Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 657 (1994).

223 *See* Cuthbertson, *supra* note 177; Jeet Heer, *Fake News Isn't the Problem*, NEW REPUBLIC (Nov. 18, 2016), https://newrepublic.com/article/138851/fake-news-isnt-problem; Craig Silverman, *This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook*, BUZZFEED NEWS (Nov. 16, 2016), https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook.

internet intermediaries can use personally identifiable information, such as persons' finances, genders, political affiliations, shopping habits, racial or ethnic characteristics, reading interests, and much more. For the internet marketplace of ideas to function more efficiently, without consumer threat from false and misleading messages, federal law should better regulate internet intermediaries' retention and dissemination of personal data.