LAWS AND TAXES AND BIG TECH, OH MY! THE CASE FOR A FEDERAL EXCISE TAX ON TARGETED DIGITAL ADVERTISEMENTS CREATED BY USE OF PERSONALLY IDENTIFIABLE DATA

INTRODUCTION

Though there is no overt subscription fee for using "free" online platforms like Facebook, it is well established there is a hidden, continuous cost: the exchange of personally identifiable information (PII) for platform use.[1] Platforms that collect PII—the best known of which include Google and Facebook—make much of their revenue by selling digital advertisements to third parties.[2] This is a common business practice, and these new digital advertisements (ads) are microtargeted, meaning an advertiser can select a minute audience with which to engage.[3] Platforms enable advertiser microselection by either matching a third-party ad to a discrete target demographic (groups created by their collection of PII)[4] or by sharing somewhat de-identified consumer data itself, usually with consumer consent (however ill informed).[5] After such an exchange,

1. Adam B. Thimmesch, *Transacting in Data: Tax, Privacy, and the New Economy*, 94 DENV. L. REV. 145, 146 (2016). The debate concerning the precise definition of PII is still raging and well beyond the scope of this Note. For simplicity's sake, this Note uses the expansive California Consumer Privacy Act (CCPA) definition of personal information: "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." CAL. CIV. CODE § 1798.140(o)(1) (West 2018).

2. *See* Matthew Johnston, *How Facebook Makes Money*, INVESTOPEDIA (Jan. 30, 2021), https://www.investopedia.com/ask/answers/120114/how-does-facebook-fb-make-money.asp [https://perma.cc/RR74-9N9Z]; *Facebook: Transparency and Use of Consumer Data: Hearing Before the H. Comm. on Energy & Com.*, 115th Cong. 47 (2018) (statement of Mark Zuckerberg, Cofounder, Chairman, and Chief Executive Officer, Facebook, Inc.).

3. *See, e.g.*, Giridhari Venkatadri et al., *Privacy Risks with Facebook's PII-based Targeting: Auditing a Data Broker's Advertising Interface*, 2018 IEEE SYMP. ON SEC. & PRIV. 89, 102 (2018) (discussing Facebook's "custom audience" feature and other PII-driven Facebook advertising methods).

4. *See, e.g.*, Brian O'Connell, *How Does Facebook Make Money? Six Primary Revenue Streams*, THESTREET (Oct. 23, 2018, 4:29 PM), https://www.thestreet.com/technology/how-does-facebook-make-money-14754098 [https://perma.cc/P2A4-EA4L] ("Facebook holds a massive amount of personal data on its user base . . . . That allows Facebook to sell advertising space to companies and organizations who want to hone in on a specific demographic, like video game players or Range Rover owners.").

5. *See, e.g.*, Kristen V. Brown, *23andMe Is Selling Your Data, But Not How You Think*, GIZMODO (Apr. 14, 2017, 5:18 PM), https://gizmodo.com/23andme-is-selling-your-data-but-not-how-you-think-1794340474 [https://perma.cc/EVM6-T6JQ]; *Your Data Is Shared and Sold . . . What's Being Done About It?*, WHARTON (Oct. 28, 2019) [hereinafter *Your Data is Shared and Sold*], https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ [https://perma.cc/6VL5-GJ96] ("[C]onsumers are often not aware all of this tracking and analysis is going on . . . . [T]hey are

advertisers reap the benefits of advertising to consumers through (generally) tax-deductible[6] targeted ads, and platforms enjoy the dual benefits of offering ostensibly free platform access to users while raking in massive profits by monetizing their information[7]—whether or not users want this.[8]

However, perhaps this system is the feature, not the bug.[9] Allowing a third-party company to use your PII to place targeted ads on your Facebook timeline seems a small price to pay while you enjoy "free" access to the lives of friends, family, and other members of your community.[10] Further, Professor Elea Feit explains that data-driven advertising enables businesses to "annoy fewer people with marketing emails because [they're] targeting folks to whom these ads are relevant."[11] Similarly, many internet users are reluctant to pay, at least *monetarily*, for access to social media platforms, and any loss of digital ad revenue could certainly have costly paywall downstream effects on the consumer.[12] Lastly, why should consumers worry about advertising, anyway?[13] Is it not a good thing that we now only see advertisements that directly appeal to us as individuals?

While there may be certain benefits to the current targeted ad regime, there are many downsides as well. First, while your PII *is* valuable, its

---

lulled into complacency . . . by the presence of a privacy policy . . . . But these policies are an exercise in 'obfuscation' . . . .").

6. *See* I.R.C. § 1.162-1(a) (West 2020). Providing, in pertinent part: "Business expenses deductible from gross income include the ordinary and necessary expenditures directly connected with or pertaining to the taxpayer's trade or business, except items which are used as the basis for a deduction or a credit under provisions of law other than section 162. . . . Among the items included in business expenses are management expenses, . . . *advertising* and other selling expenses . . . . The full amount of the allowable deduction for ordinary and necessary expenses in carrying on a business is deductible, even though such expenses exceed the gross income derived during the taxable year from such business." (emphasis added). *But see* I.R.C. § 162(e)(1)(c) for exceptions (noting there is "no deduction" for "any amount paid or incurred in connection with," among other things, "any attempt to influence the general public . . . with respect to elections").

7. *How Much Money Facebook Gets From Selling Your Data*, POPULAR MECHANICS (June 19, 2018), https://www.popularmechanics.com/technology/security/a21272151/facebook-data-money-value/ [https://perma.cc/2YZX-XPR6].

8. *See Your Data Is Shared and Sold*, *supra* note 5 (explaining that users often feel "resigned" to the current data regime).

9. *Id.* (explaining how data tracking can be beneficial). "For example, a business that knows you're a pet owner based on your searches for cat food could send you coupons." *Id.*

10. *Id.* Professor Sebastian Angel notes that society's current privacy valuation does not incentivize heavy regulation. *Id.* " 'It's really bizarre that we are unwilling to pay 50 cents for an app in the app store but we are totally okay with paying $5 or $6 for a cup of coffee,' . . . . 'Because of this psychology, it's really hard to ask people to pay for electronic things they expect to be free.' . . . Since people are unwilling to pay, 'companies have no choice but to monetize these services through things like advertising . . . .' " *Id.*

11. *Id.*

12. *See, e.g.*, Jared Walczak, *Gov. Hogan Vetoes Maryland Digital Advertising Tax Legislation*, TAX FOUND. (May 7, 2020), https://taxfoundation.org/governor-hogan-vetoes-maryland-digital-advertising-tax-legislation/ [https://perma.cc/Q65H-A727].

13. *But see* Shoshana Zuboff, *The Coup We Are Not Talking About*, N.Y. TIMES (Jan. 29, 2021), https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html

economic benefit to you is negligible; meanwhile, platforms with millions of users amass large troves of PII and profit tremendously.[14] Further, though some PII may be "worthless" to you, or at least a fair trade for free platform access, the digital targeted ad economy is so lucrative that companies are incentivized to collect PII you may otherwise desire to keep private[15]—including your "ethnicity, location, major, interests, political affiliation, purchase history, personality traits, salary, car model, browsing history," and more.[16] Even if you *do* consent to the platform's collection of your data, aggressive PII collection exposes you to the risk of massive data breaches.[17] Such breaches are notoriously hard—if not outright impossible—for the average consumer to avoid.[18] Additionally, PII can be used for more nefarious purposes than mere commercial advertising, such as negatively influencing consumer behavior,[19] widening already cavernous social equity gaps,[20] and even destabilizing democracies.[21] Finally, we must ask ourselves if hyper-personalized, targeted ads in and of themselves are *good* for us.

[https://perma.cc/S8X6-44Z7]. Zuboff worries about the future of "surveillance capitalism." *Id.* She notes that "Facebook's political advertising business is a way to rent the company's suite of capabilities to microtarget users, manipulate them and sow epistemic chaos, pivoting the whole machine just a few degrees from commercial to political objectives." *Id.*

14. *See* Johnston, *supra* note 2 (explaining Facebook makes 98% of its millions of dollars in profit from advertising); *see also* Eliana Garcés & Daniel Fanaras, *Antitrust, Privacy, and Digital Platforms' Use of Big Data: A Brief Overview*, 28 COMPETITION: J. ANTITRUST, UNFAIR COMPETITION & PRIV. L. SECTION CAL. LAWS. ASS'N. 23, 30 (2018) (discussing the various ways platforms can maximize their profits with consumer data).

15. *See, e.g.*, Nicole Martin, *How Much Does Google Really Know About You? A lot.*, FORBES (Mar. 11, 2019), https://www.forbes.com/sites/nicolemartin1/2019/03/11/how-much-does-google-really-know-about-you-a-lot/#49f7dfe17f5d [https://perma.cc/6J4U-L7YP] (discussing how much information Google can access about a user); Robert Burnson, *Google Sued for Secretly Amassing Vast Trove of User Data*, BLOOMBERG L. (June 2, 2020, 7:40 PM), https://www.bloomberglaw.com/product/blaw/document/X21V5UIG000000 (discussing a suit against Google wherein the plaintiffs allege Google collected their personal data without consent).

16. Ying Hu, *The Case for an Information Tax: Cumulative Harm in the Collective Misuse of Information,* 29 CORNELL J.L. & PUB. POL'Y 295, 302 (2019).

17. *See, e.g.*, Press Release, Federal Trade Commission, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related [https://perma.cc/588P-T24R]; Eugene Bekker, *2020 Data Breaches: The Most Significant Breaches of the Year*, IDENTITYFORCE (Jan. 3, 2020), https://www.identityforce.com/blog/2020-data-breaches [https://perma.cc/AX5A-2WXZ].

18. *See* Omri Ben-Shahar, *Data Pollution*, 11 J. LEGAL ANALYSIS 104, 145 (2019).

19. *See, e.g.*, Hu, *supra* note 16, at 312–13 (introducing a hypothetical where an individual's online behavior is tracked and manipulated by shopping websites).

20. *See, e.g.*, Deborah Raji, *How our data encodes systematic racism*, MIT TECH. REV. (Dec. 10, 2020), https://www.technologyreview.com/2020/12/10/1013617/racism-data-science-artificial-intelligence-ai-opinion/ [https://perma.cc/XEJ4-9WPN] (discussing systemic racism in programming and algorithmic development).

21. *See* Zuboff, *supra* note 13. Zuboff discusses the "consequences of this surprising political-economic fraternity as those young companies morphed into surveillance empires powered by global architectures of behavioral monitoring, analysis, targeting and prediction." *Id.* She argues that unless these major corporations are effectively regulated, we will be saddled with a surveillance society, not true democracy. *Id.*

Scholars like Shoshanna Zuboff argue that these ads, far from promoting human flourishing, do nothing more than sow "epistemic chaos," breaking down shared values in a world where "norm violation is key to revenue."[22]

The balance of privacy rights, economic equity, and fair business practices is a difficult one, and though current legal regimes have attempted to address this issue, they have come up short.[23] However, the oft-understudied field of tax law has great, untapped potential as a corrective tool.[24]

This Note explores how to preserve the positives of targeted digital advertising while correcting the negatives, using a federal digital excise tax for ads created by use of PII as an innovative solution for a digital-age dilemma. It argues the Internal Revenue Code (IRC) should be amended to deny a deduction for PII-created digital ads, and instead a new, federal excise tax should be levied on these ads. These measures might be able to disincentivize pernicious corporate data collection practices, correct platform/user economic imbalances, provide solutions to privacy harms like data breaches, and overall balance the positives of PII collection against the negatives. Section II examines the current issues with targeted digital advertising and personal data collection by examining pernicious corporate uses of data, data breaches, the use of PII to perpetuate economic inequality, and the inability of the individual to stop these harms. Section III details the successes and failures of current legal regimes in addressing the aforementioned issues. Section IV proposes that, by disallowing a tax deduction for PII-created targeted advertising *and* implementing an excise tax on such advertising, tax law provides a practical remedy to the issues described in Section II. Finally, Section V discusses criticisms of such a tax, specifically addressing how it could be constitutional even under the

22. *Id.* For more on "flourishing" and well-being, see Roger Crisp, *Well-Being*, STAN. ENCYC. PHIL. (Edward N. Zalta ed., 2017), https://plato.stanford.edu/entries/well-being/ [https://perma.cc/8LUA-FMQP].

23. *See* discussion *infra* Section III.

24. *See* Thimmesch, *supra* note 1, at 145. *See generally* Christian Fuchs*, The Online Advertising Tax: A Digital Policy Innovation*, CAMRI Policy Briefs (2018), https://westminsterresearch.westminster.ac.uk/download/e95e51dbf2d39eb8340905241eed9895d132769f679b705bae8bc2dfe5872235/325199/the-online-advertising-tax.pdf (outlining tax policy options as they relate to digital advertising).

exacting commercial speech standard in *Sorrell v. IMS Health Inc*.[25] The digital world is already here—digital taxes should not be far behind.

I. TARGETED DIGITAL ADVERTISING AND HARM

A. What is Targeted Digital Advertising?

It is no surprise advertisers want to know how people think—after all, the entire purpose of the advertising industry is to convince consumers to buy a product. In the recent years[26] of the digital revolution, there has been an explosion of hyper-personalized, targeted online advertising.[27] However, businesses have always courted consumers;[28] what makes this new type of advertising so particularly harmful?

All ads are somewhat targeted.[29] For example, an ad for a cancer treatment is aimed at those seeking such a treatment, and an ad for a Missouri-barred lawyer will likely be aimed at Missouri residents with Missouri legal problems.[30] While it is true all advertising involves appealing to a purchaser, most early twentieth century ads were *passive*; the content and placement of such ads were largely independent of the individual consumer.[31] Rather, these ads targeted broad demographics, usually limited

25. 564 U.S. 552 (2011).

26. *See* Dolly Bagnall, *The History of Online Advertising: From the First Banner Ad to Everything That's Happened Since*, OKO AD MGMT. (July 19, 2019), https://oko.uk/blog/the-history-of-online-advertising [https://perma.cc/6UMR-26CB]; Roy de Souza, *A Short History of Targeted Advertising*, ZEDO (May 27, 2015), https://www.zedo.com/short-history-targeted-advertising/ [https://perma.cc/K6LP-E8BF].

27. So much so that some Facebook users have made a game out of "tricking" the algorithm in hopes of being shown weird, nonsensical ads. *See* Morgan Sung, *It Turns Out Purposely Messing with Your Targeted Ads Isn't a Good Idea*, MASHABLE (Apr. 26, 2019), https://mashable.com/article/purposely-engaging-with-weird-ads-isnt-good/ [https://perma.cc/7NNQ-V9JB] (writer explaining how she intentionally clicked on relevant ads and search inquiries in order to get "my ads to show me extremely specific cephalopod-shaped home decor").

28. William M. O'Barr, *A Brief History of Advertising in America*, 6 ADVERT. & SOC'Y REV. (2005), https://muse.jhu.edu/article/193868#fig02 [https://perma.cc/9NHL-XXRP]; *see also* Daniel E. Troy, *Advertising: Not "Low Value" Speech*, 16 YALE J. ON REG. 85, 97 (1999) (discussing advertising in colonial America).

29. Bertel King, *Why Targeted Ads Are a Serious Threat to Your Privacy*, MAKE USE OF (Apr. 1, 2019), https://www.makeuseof.com/tag/targeted-ads-threat-privacy/ [https://perma.cc/9X3D-EY64].

30. Indeed, if the ad was run in other states the attorney might face ethical issues. *See* JOHN S. DZIENKOWSKI, PROFESSIONAL RESPONSIBILITY: STANDARDS, RULES, AND STATUTES 84–87 (2019–2020 ed., 2019).

31. *See* de Souza, *supra* note 26; *see also* Gillian B. White, *When Algorithms Don't Account for Civil Rights*, ATLANTIC (Mar. 7, 2017), https://www.theatlantic.com/business/archive/2017/03/facebook-ad-discrimination/518718/ [https://perma.cc/N5LE-CJ5H] (noting that Doc Searls, "founder of ProjectVRM at Harvard, which works on issues of standards and protocols for technology" is concerned about Facebook's incessant data mining, saying "An important thing about advertising of the traditional kind . . . is that it's not personal. It's aimed at large populations. . . . The profiling was pretty minimal, and it was never

to "age, sex, and income."[32] There were exceptions—aggressive "ambulance-chasing" legal solicitation, for example[33]—but such exceptions were rare; generally, there was no way to target a *particular* consumer.[34] This all changed with the 1970s' explosion of psychographics, the study of consumer "lifestyle" data including political leanings, sexual preference, and medical information, among other data sets.[35] Even with this information influx, advertisers did not generally rely on personal information provided *by* the individual consumer to place ads; rather, they made educated guesses about what *kind* of person was watching the Travel Channel or reading *Ladies' Home Journal* and ran ads for plane tickets and irons in each medium, respectively.[36] With the advent of cable, advertisers further refined their strategies, and as "[b]roadcasting became narrowcasting," advertising followed suit.[37] Though advertisers were able to narrow down their consumer base more accurately than ever before, they still did not know about *you*, the entire individual, only you, one member of the group of people that routinely watches *Full House*.[38] Now, in the internet age, it takes advertisers (or platforms)[39] only a few clicks to learn all about *you* the individual:[40] your location; other websites you have visited; immense information about your health, finances, marital status; and even

personal."). *But see* O'Barr, *supra* note 28 (arguing that ancient advertising practices were much more personal than twentieth century mass-media advertising).

32. de Souza, *supra* note 26; *see also* O'Barr, *supra* note 28 ("Mass media began to decline with the advent of cable television in the 1970s. Until then, viewing options were limited and audiences were broad.").

33. *See, e.g.*, Fla. Bar v. Went For It, Inc., 515 U.S. 618, 635 (1995) (holding that the Florida Bar could constitutionally regulate certain types of targeted legal solicitation under Commercial Speech doctrine).

34. *See* White, *supra* note 31 and accompanying text.

35. de Souza, *supra* note 26; *see also* Mark Bartholomew, *Advertising and the Transformation of Trademark Law*, 38 N.M. L. REV. 1, 31 (2008).

36. *See* de Souza, *supra* note 26 (discussing how advertisers tried to target niche markets by positioning "a product in the marketplace to attract the psychographic to which the brand appealed").

37. O'Barr, *supra* note 28. *But see* J. Howard Beales, III, *Advertising to Kids and the FTC: A Regulatory Retrospective That Advises the Present*, 12 GEO. MASON L. REV. 873, 875 (2004) (noting substantial regulation of advertising targeting children).

38. *See* White, *supra* note 31.

39. Advertising agencies are also now being displaced, with digital platforms and content-driven websites now moving their advertising functions in-house. *See* Mike Shields, *The Future of Ad Agencies Has Never Been More in Doubt*, BUS. INSIDER (Jun. 18, 2017, 12:17 PM), https://www.businessinsider.com/companies-are-cutting-out-ad-agencies-and-going-in-house-2017-6 [https://perma.cc/2LNM-U2AB] ("Facebook and Google are raking in a disproportionate amount of new ad spending, and both are building more agency-like functionality. Companies like Vice and BuzzFeed are making content for marketers and distributing it.").

40. Rebecca Walker Reczek, Christopher Summers & Robert Smith, *Targeted Ads Don't Just Make You More Likely to Buy—They Can Change How You Think About Yourself*, HARV. BUS. REV., (Apr. 4, 2016), https://hbr.org/2016/04/targeted-ads-dont-just-make-you-more-likely-to-buy-they-can-change-how-you-think-about-yourself [https://perma.cc/R6TC-24LK] ("Thanks to online tracking technology, marketers no longer have to rely on assumptions about consumer behavior. Instead, they can deliver ads targeted specifically to individuals based on their behavior online.").

how you feel at a particular moment.[41] This is today's targeted advertising: microtargeted digital advertising that uses an individual's PII to aggressively appeal to the user.[42] Additionally, today's digital advertising is reaching more people than ever—as of 2018, Americans consume five times more information than they did fifty years ago,[43] and most of that information is mediated through screens.[44] Given the proliferation of this ubiquitous new advertising, we must familiarize ourselves with the medium's negatives and positives.

B. Are Targeted Ads Harmful?

Digital targeted ads, though perhaps ostensibly innocuous, lie at the heart of a heated debate over the intersections of privacy and capitalism,[45] autonomy and coercion.[46] This Note aims to explain why the harms of *unrestrained* targeted digital advertising outweigh the benefits.

Beginning with the benefits, digital targeted ads are more relevant to our interests because they expose us to products we are more likely to want.[47] Second, free platform use depends heavily on these ads.[48] For example, Spotify offers an "ad-free" premium membership for nine dollars and ninety-nine cents.[49] At first glance, this implies that the consumer who does not opt in to the "ad-free" membership is willing to watch targeted ads created by use of their PII[50] for free platform access.[51] Any attempt to stymie

41. *See* Ruth Reader, *Spotify Wants to Monetize Your Mood with Ads Based on your Favorite Playlists*, VENTURE BEAT (Apr. 16, 2015, 10:45 AM), https://venturebeat.com/2015/04/16/spotify-wants-to-monetize-your-mood-with-ads-based-on-your-favorite-playlists/ [https://perma.cc/3B8W-686M]; *see also* Martin, *supra* note 15; Lina M. Khan, *Sources of Tech Platform Power*, 2 GEO. L. TECH. REV. 325, 329 (2018).

42. *See* Joseph Newman, *Cookie Monsters: Locally Stored Objects, User Privacy, and Section 1201 of the DMCA*, 41 AIPLA Q.J. 511, 513–17 (2013).

43. Nicole F. Roberts, *How Much Time Americans Spend in Front of Screens Will Terrify You*, FORBES (Jan. 24, 2019, 2:24 AM), https://www.forbes.com/sites/nicolefisher/2019/01/24/how-much-time-americans-spend-in-front-of-screens-will-terrify-you/?sh=28d44a391c67 [https://perma.cc/4XNA-YU7K].

44. Chris Ritter, *Technology and Mental Health: How Lawyers Are Affected by Devices and Social Media and What to Do About It*, 82 TEX. B.J. 598 (2019) (noting Americans, on average, spend over ten hours a day staring at screens).

45. *See* Zuboff, *supra* note 13.

46. *See* Hu, *supra* note 16, at 302.

47. *See Your Data Is Shared and Sold, supra* note 5 ("With more information about a person, a business can send ads to people who are more likely to buy or use the service.").

48. *See supra* text accompanying notes 1 and 10–11.

49. *Get Premium Free for 1 Month*, SPOTIFY, https://www.spotify.com/us/premium/ [https://perma.cc/768L-NWFF].

50. *See* Liz Pelly, *Big Mood Machine*, BAFFLER (June 10, 2019), https://thebaffler.com/downstream/big-mood-machine-pelly [https://perma.cc/3EGD-3L6D] (discussing Spotify's use of "mood" playlists when placing advertisements).

51. This is not to say Spotify does not *collect* user data from Premium accounts. They do. *See* Daniel Terdiman, *Spotify Exec: We Collect an 'Enormous Amount of Data on What People are Listening*

or heavily regulate targeted ads might reduce the ability of customers to make this choice, or worse, pass the cost onto consumers, forcing everyone to pay nine dollars and ninety-nine cents even if they were perfectly happy with the original arrangement.[52] In the business world, many have argued that regulating, forbidding, or heavily taxing digital advertising would irrevocably harm small businesses that rely on ads to support their websites or reach new customers—especially during a global pandemic.[53] For example, in response to a proposed Maryland tax on digital advertising, opponents argued that

> It's not just Fortune 500 companies that advertise online, it's your local barber, your local auto mechanic, your local watering hole and those critical nonprofits. [A tax on digital advertising] would raise taxes and the cost of doing business for all these hardworking Marylanders and the ripple effect is obvious: higher taxes, higher prices, fewer jobs. . . . Under COVID-19, the impacts of the fiscal pressures on our small businesses and nonprofits have been catastrophic. . . . Now is NOT the time to increase the cost of doing business, especially with online ad sales.[54]

To summarize, the main anti-regulation arguments are (1) consumers should have the freedom to "choose" which PII they are willing to (implicitly) trade for platform use and (2) economic benefits outweigh potential privacy-related negatives.

As for the negatives, this argument flips. Targeted digital ads are harmful for many reasons, but this Note will focus on four issues: (1) they incentivize platforms to engage in pernicious, invasive data practices against the best interests of users; (2) corporate data collection exposes user PII to the risk of massive data breaches; and (3) the value that platforms and advertisers extract from the user PII far outstrips the initial "value" the data has in consumers' hands, creating a massive economic imbalance in favor of a small number of large platforms. Finally, an underlying thread in all of the above issues is that (4) users cannot meaningfully avoid *any* of the

---

To, Where, and in What Context', VENTURE BEAT (Feb. 24, 2015, 1:27 PM), https://venturebeat.com/2015/02/24/spotify-exec-we-collect-an-enormous-amount-of-data-on-what-people-are-listening-to-where-and-in-what-context/ [https://perma.cc/46K7-LK3T]. Further, brands can still promote "branded" playlists, which are visible on both premium and non-premium accounts. *Id.*

52. *See, e.g.*, Rick Weldon, *The Dark Side of the Digital Advertising Tax & How It Could Affect You*, FREDERICK CHAMBER INSIGHTS (last visited Apr. 15, 2021), https://frederickchamberinsights.com/2020/12/10/the-dark-side-of-the-digital-advertising-tax-how-it-could-affect-you/ [https://perma.cc/MRT5-RTW8].

53. *See, e.g.*, *id.*

54. *Id.*

aforementioned problems simply by "choosing" better platforms; there is no meaningful "opt-out."[55]

1. Platforms' Pernicious Data Practices

When discussing PII collection harms, most people think less about commercial advertisements and more about incidents like Facebook's 2018 Cambridge Analytica debacle.[56] The Trump 2016 campaign hired a political data firm, Cambridge Analytica, to provide data on voter preferences so the campaign could work to influence American voters.[57] To do so, Cambridge Analytica provided a personality test that Facebook users took on a downloaded app; however, after users downloaded the app, it "scraped some private information from their profiles and those of their friends."[58] Though only 270,000 users actually consented to this data collection (and even then, they were told their data would be used only for academic purposes), over fifty million discrete user profiles were created from the scraped data.[59] This happened because "a loophole in Facebook's [application programing interface] . . . allowed third-party developers to collect data not only from *users* of their apps but from all of the people in those users' *friends* network on Facebook."[60] Additionally, far from being anonymized as originally promised,[61] these discrete, identifiable profiles were used to create targeted digital political ads.[62] Though Facebook has since banned this type of "data scraping," and Cambridge Analytica alleges the researcher who created the profiles violated Facebook's data use rules, the damage is done: once user

55. *See Your Data Is Shared and Sold*, *supra* note 5 (computer and information science professor, Sebastian Angel, claiming "[t]here's no real way to opt out").

56. Joseph T. McClure, *A New Trend in Securities Fraud: Punishing People Who Do Bad Things*, 48 TEX. J. BUS. L. 28, 42–43 (2020) (discussing consumer outrage at Facebook's decision to let Cambridge Analytica harvest user data without user consent).

57. Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [https://perma.cc/Z4UN-F288].

58. *Id.*

59. *Id.*

60. Aja Romano, *The Facebook Data Breach Wasn't a Hack. It was a Wake-Up Call.*, VOX (Mar. 20, 2018, 4:50 PM), https://www.vox.com/2018/3/20/17138756/facebook-data-breach-cambridge-analytica-explained [https://perma.cc/T77X-YDC8] (emphasis added).

61. *See* Phillip Bump, *Everything You Need to Know About the Cambridge Analytica-Facebook Debacle*, WASH. POST (Mar. 19, 2018, 10:14 AM), https://www.washingtonpost.com/news/politics/wp/2018/03/19/everything-you-need-to-know-about-the-cambridge-analytica-facebook-debacle/ [https://perma.cc/N5TV-3J6K].

62. *See* Granville, *supra* note 57. For other political campaigns that used Cambridge Analytica, see Patrick Svitek & Haley Samsel, *Ted Cruz Says Cambridge Analytica Told His Presidential Campaign Its Data Use Was Legal*, TEX. TRIB. (Mar. 20, 2018, 2:00 PM), https://www.texastribune.org/2018/03/20/ted-cruz-campaign-cambridge-analytica/ [https://perma.cc/BT9J-5V3A] (explaining Ted Cruz's presidential campaign worked with Cambridge Analytica).

data is out there, it is difficult to erase.[63] Even more concerning is how this PII, once collected, can be *used*. The more data platforms collect, the more effective and targeted their ads may be and the more they profit.[64] However, this efficiency has costs, privacy being one of the greatest[65]—the tradeoff for more effective ads is less consumer privacy and more consumer manipulation.[66]

a. Data Collection

Most people value privacy.[67] The existence of nondisclosure agreements,[68] doctor-patient confidentiality,[69] and constitutional jurisprudence[70] all evince a longstanding cultural commitment to privacy protection. However, with more advanced technology than ever before, it is terribly difficult to regulate privacy, and scholars worry about newfound "unprecedented abilities to collect personal data," because "technological developments suggest that costs of data collection and surveillance will decrease, while the quantity and quality of data will increase."[71] Consumer privacy is particularly lacking,[72] and this has shined a spotlight on the lack of individual privacy rights in general.[73] The U.S. response, at least

63. Granville, *supra* note 57.

64. See Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1379–80, 1420–21 (2017) for a brief overview of this process and a discussion of data monetization.

65. *See generally* Kenneth A. Bamberger, Serge Egelman, Catherine Han, Amit Elazari Bar On & Irwin Reyes, *Can You Pay for Privacy? Consumer Expectations and the Behavior of Free and Paid Apps*, 35 BERKELEY TECH. L.J. 327 (2020).

66. *See, e.g.*, Hu, *supra* note 16, at 312 (discussing a platform user manipulation hypothetical).

67. *See* Jeff Sovern, *Opting in, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1052–58 (1999).

68. *See* Alexandra Twin & Khadija Khartit, *Non-Disclosure Agreement (NDA)*, INVESTOPEDIA (Jan. 3, 2021), https://www.investopedia.com/terms/n/nda.asp [https://perma.cc/X6HN-JCPJ].

69. *See What You Need to Know About Breaches in Doctor-Patient Confidentiality*, WILSON KEHOE WININGHAM (Jun. 27, 2020), https://www.wkw.com/indianapolis-medical-malpractice-lawyers/blog/doctor-patient-confidentiality/ [https://perma.cc/ZDS3-UZSE].

70. *See* U.S. CONST. AMEND. IV; Griswold v. Connecticut, 381 U.S. 479, 484 (1965) ("[S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. . . . Various guarantees create zones of privacy.").

71. A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1463 (2000).

72. *See* Bennet Cyphers, *Google Says It Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits It*, ELEC. FRONTIER FOUND. (Mar. 19, 2020), https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and [https://perma.cc/KD6A-63KH]; Wes Schlagenhauf, *Spotify Turns Our Emotions into Data, and then Profits Off of Them*, HUSTLE (June 12, 2019), https://thehustle.co/spotify-turns-emotions-into-data/ [https://perma.cc/UB6X-TGLU].

73. *See* Alessandro Acquisti, Leslie K. John & George Loewenstein, *What Is Privacy Worth?*, 42 J. LEGAL STUD. 249, 251 (2013). Users are also voicing concerns about government misuse of PII, but that is beyond the scope of this paper and worthy of an investigation all its own. *Id.*

federally,[74] has centered not on protecting digital privacy as an inherent right[75] but as a contractual agreement—meaning as long as users have contractual "notice and choice," PII collection is allowed.[76] Despite the ostensible benefit of freedom to contract, the Americanized "notice and choice" model does not truly give users notice *or* choice; but it does give invasive PII collection an air of legitimacy.[77] First, by characterizing platform/user PII "exchanges" as free and contractual, the government ignores the bargaining power inequity between unsophisticated, individual users and large, complex corporations.[78] Second, platforms take advantage of this sham bargaining equality by routinely hiding their privacy-eroding practices behind manipulative policies.[79] Researchers Neil Richards and Woodrow Hartzog ask users to examine this "notice and choice" regime:

> Think about your own agreements with the social networks you use, the apps you install on your phone, or the Amazon Alexa that might sit, listening, in your kitchen or bedroom. Do you know what you agreed to? Have you read the agreements? Did you have a meaningful choice? While the answer to these questions is usually "no," the dominant legal regime that applies in the United States is that the terms and conditions of these services are valid as long as there is some kind of "notice and choice" to consumers. In practice, and as enforced with occasional exception by the Federal Trade Commission (FTC), notice-and-choice models can be legally sufficient even if the notice is buried somewhere in a dense privacy policy, and the choice is take-it-or-leave-it—accept what a company wants to do with your data or not use the service at all.[80]

Third, even if there is an opt-out option, it is usually obscure and manipulative.[81] Additionally, the downstream opt-out cost falls on the user,

---

74. State responses have varied greatly. *See California Consumer Privacy Act (CCPA)*, OFF. ATT'Y GEN., https://oag.ca.gov/privacy/ccpa [https://perma.cc/L4GL-TAEV]; *State Laws Related to Internet Privacy*, NAT'L CONF. OF STATE LEGISLATURES (Jan. 17, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx [https://perma.cc/BCH6-NP9Y].

75. *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1727 (2020) [hereinafter *Privacy's Constitutional Moment*] ("The American constitutional system has no explicit constitutional right to privacy."). However, "[t]he European Convention on Human Rights has long been held to protect a right to privacy." *Id.* This includes some rights to data privacy under the General Data Protection Regulation. *Id.* at 1727–28.

76. *Id.* at 1734.

77. *See id.*

78. *See* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1487–88 (2019) [hereinafter *Pathologies of Digital Consent*].

79. *See Privacy's Constitutional Moment*, *supra* note 75, at 1734.

80. *Pathologies of Digital Consent*, *supra* note 78, at 1463 (footnotes omitted).

81. *Your Data Is Shared and Sold*, *supra* note 5. *See also Pathologies of Digital Consent*, *supra* note 78, at 1489. The article explains that

generally forcing them to "pay for privacy."[82] Fourth, as Cambridge Analytica demonstrates, even if the user goes through this costly, time-consuming process and succeeds in opting out, if someone connected to them does not, their PII may still be up for grabs.[83] This is a theme of the current U.S. privacy policy regime—placating users without providing them any meaningful control over their PII.[84] In the end, you have little control over who knows what about you and how.[85]

b. Data Manipulation

Targeted digital advertisements serve this surveillance regime in two ways: first, they incentivize platforms to monetize consumer data, even though consumers may not desire this,[86] and second, they use this data to manipulate consumer behavior by placing the targeted ads.[87] To the first point, increased PII collection makes better ads, and better ads make more *money*—which, as seen above, is how most platforms make their profits.[88] To the second point, despite having heretofore unheard-of access to sensitive, private data, there are few U.S. regulations in place that tell corporations how to protect or ethically handle data.[89] Rather, corporations are mostly left to their own devices and handle data by way of their profit motive, with little regard to other values[90]—and Section 230 of the Communications Decency Act enables them to do so.[91] One need not look

---

> [C]ompanies have strong incentives to obtain consent, . . . [and] many of these malicious interfaces are used to . . . manipulate people to grant it. Examples ranging in severity abound. . . . Consider the concept of what Brignull calls 'confirmshaming,' that is, 'the act of guilting the user into opting into something. The option to decline is worded in such a way as to shame the user into compliance.' Consider the request from MyMedic to send users notifications, which forces those who do not wish to receive notification to click a button labeled 'no, I prefer to bleed to death.' It's a subtle form of psychological coercion, but at scale these attempts can deplete our resolve.

Id. (footnotes omitted).

82. *See* Bamberger, *supra* note 65, at 328.

83. *See supra* text accompanying note 56.

84. *See Pathologies of Digital Consent*, *supra* note 78, at 1472.

85. *See* Zuboff, *supra* note 13.

86. *See* Elvy, *supra* note 64, at 1386–87, 1406 (citing a survey that "indicates that consumers would not willingly choose to sacrifice their privacy in exchange for targeted advertising" (internal quotation marks omitted)); *see also Your Data is Shared and Sold*, *supra* note 5, *and* Hu, *supra* note 16, at 302–04.

87. *See* Hu, *supra* note 16, at 312.

88. *See* Johnston, *supra* note 2 and accompanying text.

89. *See Privacy's Constitutional Moment*, *supra* note 75, at 1697.

90. *Id.* at 1726. "If the United States embraces a narrow view of data protection, it will remain agnostic to these costs at this pivotal moment and instantiate a system that seeks for maximum exposure (and profit) with little thought to collateral harm and social good." *Id.*

91. Platforms rely on Section 230(c) (colloquially "Section 230") of the Communications Decency Act to avoid liability for failing to stop malicious posts. *See* Daisuke Wakabayashi, *Legal Shield for Social Media Is Targeted by Lawmakers*, N.Y. TIMES (May 28, 2020),

far to see the effects of this unrestrained, market-driven self-regulation.[92] In particular, not only have hypertargeted online advertisements funded the platforms that spread, or fail to stop, malignant disinformation and hate speech, but they have become weapons themselves.[93] For example, Facebook enabled advertisers to target users who searched hate speech terms—if collection of search data were strictly limited, it is unlikely this weaponized advertising could have occurred.[94] Additionally, advertisements (and the algorithms that place them) can cement social inequities in a digital context.[95] For example, the National Fair Housing Alliance recently sued Facebook for an alleged violation of the Fair Housing Act.[96] Plaintiffs claimed that "Facebook's advertising platform enabled landlords and real estate brokers to prevent protected classes from receiving housing ads" by targeting ads in a discriminatory fashion.[97] Facebook's algorithm seeks to "maximize" advertiser return by using consumer data to

https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html [https://perma.cc/V33J-BT4X]. Wakabayashi explains that "Section 230 shields websites from liability for content created by their users. It permits internet companies to moderate their sites without being on the hook legally for everything they host. It does not provide blanket protection from legal responsibility for some criminal acts, like posting child pornography . . . ." This "liability protection . . . extends to fringe sites known for hosting hate speech, anti-Semitic content and racist tropes . . . ." *Id. See also* 47 U.S.C. § 230. Section 230(c)(1) states "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." *Id.* For an overview of platforms using Section 230 to avoid liability, particularly regarding online sexual harassment, *see generally* Danielle Keats Citron & Benjamin Wittes*, The Problem Isn't Just Backpage: Revising Section 230 Immunity*, 2 GEO. L. TECH. REV. 453 (2018).

92. *See, e.g.*, Kalev Leetaru, *Should Social Media Be Allowed to Profit from Terrorism and Hate Speech?*, FORBES (Dec. 14, 2018, 10:31 PM), https://www.forbes.com/sites/kalevleetaru/2018/12/14/should-social-media-be-allowed-to-profit-from-terrorism-and-hate-speech/?sh=3a8f02e492c8 [https://perma.cc/VXV9-REJH]. "When racist, sexist, anti-Semitic and all other forms of hate speech are posted, . . . [platforms] earn[] a profit from the ads shown alongside them. . . . [T]he most horrific and harmful content posted to social media directly monetarily benefits the platforms by earning them advertising revenue." *Id.*

93. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 509 (2018) [hereinafter SURVEILLANCE CAPITALISM].

94. *See id.* at 510.

95. *See* Harris Mateen, Book Note, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, 39 BERKELEY J. EMP. & LAB. L. 285, 286 (2018) (reviewing CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016)).

96. Nadiyah Humber & James Matthews, *Fair Housing Enforcement in the Age of Digital Advertising: A Closer Look at Facebook's Marketing Algorithms*, BOSTON BAR J., Winter 2020, at 38.

97. *Id.*

exclude or include individuals—which can have a negative disparate impact on marginalized groups.[98]

In addition, the ads we see affect our behavior on an individual level, however slightly. Consider researcher Ying Hu's hypothetical:

> John starts to experience onset of bipolar disorder in his early twenties. . . . [H]e goes on a shopping spree when he suffers from a significant mood swing. Shopping websites, while unaware of his illness, notice that John is 300% more likely to purchase products during certain times, and especially after he has been to a pub or goes home late. They therefore start to collect publicly available information about John's locations and follow him on social media. Whenever John has been to a pub or has been active online late at night, these websites will serve more advertisements to him about luxury products. Unable to resist the temptation, John finds himself spending most of his money on luxury items that he does not need. . . .
>
> . . . .
>
> John has been searching for more information about bipolar disorder online and sharing his symptoms in public discussion forums. Since then, he starts to receive more advertisement both online and offline about products that claim to "cure" bipolar disorder. Since he has not shared [this] with his colleagues, John finds it highly embarrassing when one of his colleagues sees a Google ad about bipolar disorder on his computer screen. . . .
>
> . . . .

98. *Id.* at 41 (citing Conn. Fair Hous. Ctr. v. Corelogic Rental Prop. Sols., LLC, 369 F. Supp. 3d 362 (D. Conn. 2019)). The court in *Connecticut Fair Housing*

> found that plaintiffs had pled sufficient facts to establish a causal connection between a tenant screening company's alleged activity and unlawful housing denials to support a claim of disparate impact based on race. The court found that the defendant had created and provided the automated screening process, suggested the categories by which the housing provider could screen potential tenants, made eligibility determinations, and sent out letters to potential tenants notifying them of these decisions.

Id. (citations omitted).

> . . . It is not until much later that John becomes aware of an online report about him that highlights his propensity to engage in impulse shopping and concludes that he might suffer from some mental illness. In addition, John receives a much higher quote for medical insurance than most men of his age. . .[99]

While pushed to the extreme, Hu's hypothetical is not out of the realm of possibility.[100] Platforms exist to maximize their profits, and they are not above manipulating consumers through addictive interfaces to convince them to act against their best interests.[101] However, platform misuse of PII is not the only concern we must face.

2. Data Breaches

Data breaches are one of the more identifiable ills of the data economy, and various courts and agencies have begun to recognize this new harm.[102] Still, though public regulations like the Fair Credit Reporting Act (FCRA) regulate PII storage and, consequently, breaches of that storage, these statutes cover only narrow amalgamations of data.[103] Furthermore, even if the PII is stolen from one of the covered entities, it can be difficult for users to meet standing requirements by alleging a cognizable injury in fact.[104] Users often struggle to prove that they were *in fact* harmed by the data breach, as many data breach harms are intangible and far reaching.[105] How do you prove a distant breach of information led to a particular future harm like identity theft?[106] Even if the breach can be traced back to that particular

99. Hu, *supra* note 16, at 312–13 (footnotes omitted).

100. *See id.* at 302 (providing "anecdotal evidence of how someone managed to create a three-week long secret Facebook ad campaign that targeted only one person, his roommate, which was so personal and accurate that it drove his roommate 'to a state of paranoia' at a cost of merely $1.70.").

101. *See Privacy's Constitutional Moment*, *supra* note 75, at 1756–57.

102. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 747 (2018).

103. *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 255 (2007).

104. See generally Michael B. Jones, *Uncertain Standing: Normative Applications of Standing Doctrine Produce Unpredictable Jurisdictional Bars to Common Law Data Breach Claims*, 95 N.C. L. REV. 201 (2016) for an explanation of the courts' muddled approach to data breach standing issues.

105. *See, e.g.*, Paul v. Providence Health Sys. Or., 273 P.3d 106, 111 (Or. 2012) (holding "the cost of monitoring to protect against an increased risk of harm—in the absence of present injury—is not recoverable in a negligence action"). *But see* James Bogan III, *Data Breach Class Actions: Second Circuit Sets Out Parameters for Article III Injury-in-Fact*, JD SUPRA (June 1, 2021), https://www.jdsupra.com/legalnews/data-breach-class-actions-second-5007526/ (describing the Second Circuit's decision in McMorris v. Carlos Lopez & Associates, LLC, 995 F.3d 295 (2d Cir. 2021) as potentially "the most useful circuit decision to date on the injury-in-fact issue, as it provides a workable framework for standing that likely will be applied in data breach cases for years to come").

106. *Providence Health*, 273 P.3d at 110.

hack, unless you can prove the thief *harmed* you, the platform will not be liable.[107] In other words, "*future* injury is too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.' "[108]

Additionally, if an administrative agency punishes the violating company, such punishments are usually in the form of an individualized settlement, meaning there is no precedential value going forward.[109] The Federal Trade Commission's (FTC) consent decrees demonstrate this issue. Though some have argued these *do* create a "common law of privacy,"[110] technically only the companies with which the FTC negotiates are bound by each decree.[111] Additionally, the FTC has broad prosecutorial and enforcement powers,[112] but it does not always have the means to prosecute smaller "bad actors," so individualized harms might go unaddressed for the sake of prosecuting larger, more influential companies.[113] Finally, data breaches, whether by negligence or targeted theft, are generally considered inevitable.[114] While these breaches are arguably a form of digital pollution (and therefore a public nuisance),[115] both private and public law have yet to

107. *Id.* "Assuming . . . that defendant owed a duty to protect plaintiffs against economic losses, we nevertheless conclude . . . that plaintiffs' allegations here are insufficient because plaintiffs do not allege actual, present injury caused by defendant's conduct." *Id.*

108. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013) (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

109. Crystal N. Skelton, *FTC Data Security Enforcement: Analyzing the Past, Present, and Future*, 25 COMPETITION: J. ANTITRUST, UCL & PRIV. SECTION STATE BAR CAL. 305, 312 (2016) (discussing Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015)).

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

111. *See* Jean Murray, *How a Consent Decree Works and When It's Used*, BALANCE SMALL BUS. (Sept. 25, 2020), https://www.thebalancesmb.com/what-is-a-consent-decree-how-does-it-work-4580322 [https://perma.cc/G3UA-XK4M].

112. *See Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N (May 2021), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/4QF4-8NPQ].

113. This uncertain discretion is frustrating for individuals and corporations alike. *See* John Schinasi, *Practicing Privacy Online: Examining Data Protection Regulations Through Google's Global Expansion*, 52 COLUM. J. TRANSNAT'L L. 569, 601–02 (2014) (expressing frustration that the "FTC did not prosecute a single company for violating the Safe Harbor protections to E.U. citizens' privacy" between 2004 and 2009); Geoffrey A. Manne & Kristian Stout, *When "Reasonable" Isn't: The FTC's Standardless Data Security Standard*, 15 J.L. ECON. & POL'Y 67, 82 (2019) (explaining corporate frustration that "[t]here is no . . . certainty with respect to FTC enforcement of Section 5. . . . [T]he FTC seeks targets for investigation and exercises prosecutorial discretion without disclosure of the basis upon which it does so.").

114. *See, e.g.*, Charles Rust, *Against the Wind: Have We Accepted Data Breach As an Inevitability?*, 43 N. KY. L. REV. 87, 100 (2016).

115. *See* Ben-Shahar, *supra* note 18, at 129. Ben-Shahar proposes that "[d]igital information is the fuel of the new economy." *Id.* at 104. Recognizing that data, like oil, pollutes, he explains "[h]armful 'data emissions' are leaked into the digital ecosystem, disrupting social institutions and public interests" and develops "a novel framework—data pollution—to rethink the harms the data economy creates and the way they have to be regulated." *Id.* Rejecting a personal privacy-centric framework, he declares "a central problem in the digital economy has been largely ignored: how the information given by people

provide an effective solution. Users, unless they go off the grid entirely,[116] have no way to avoid these issues. And even off the grid, users cannot control the data that connects them to *other* people online.[117]

3. Untaxed Platform Profits

There is nothing wrong with a profitable business model; however, it has long been recognized as wrong to profit unjustly "at the expense of another."[118] Though much ink has been spilled over *harms* cause by privacy losses, relatively little attention has been turned to platforms' wrongful *gains*.[119] As shown above, it is well established that personal data has some sort of monetary value.[120] However, the value of one individual's PII is generally negligible—or at least difficult to price.[121] But advertising sales based on personal data are quite valuable in *aggregate*, and many Big Tech corporations craft their business models around data monetization.[122] The average consumer often has no idea their data has value; even if they *are* aware, PII is valuable in aggregate, which means one person selling their data is at a huge disadvantage compared to a large company selling troves

---

affects others, and how it undermines and degrades public goods and interests" and says his pollution framework can focus "on controlling these external effects" by using "tools used to control industrial pollution—production restrictions, carbon tax, and emissions liability." *Id.*

116. *But see* Carolyn Gray, *Who Pays the Price? Regulation of Data Tracking and Online Behavioral Advertising*, 8 ARIZ. SUMMIT L. REV. 385, 401 (2015) (discussing expensive "off-the-grid" phones, and noting that even then, these phones do not stop the overarching data brokering issue).

117. *See supra* text accompanying note 55.

118. *See* RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 1 (West 2011). Unjust enrichment is not the only way one might unjustly profit at another's expense. *See also* Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1030 (N.D. Cal. 2012) (discussing conversion and breach, among other causes of action); Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 803 (N.D. Cal. 2011) (discussing California's codification of the "misappropriation" tort).

119. *See* Bernard Chao, *Privacy Losses as Wrongful Gains*, 106 IOWA L. REV. 555 (2021) (suggesting "privacy victims should use the often-misunderstood law of restitution and unjust enrichment to disgorge wrongful gains companies earn when they break their privacy policies" because "unjust enrichment focuses on the defendant's wrongful gain and not the plaintiff's injury" therefore avoiding "many of the pitfalls associated with the more common causes of action privacy plaintiffs typically raise").

120. Robin Bloor, *How Much is Your $$$Data Worth?*, MEDIUM (Mar. 21, 2018), https://medium.com/permissionio/how-much-is-your-data-worth-c28488a5812e [https://perma.cc/469W-E42T]. *See supra* text accompanying note 7.

121. *See* Thimmesch, *supra* note 1, at 174–77; *But see* Bloor, *supra* note 120. *See also* Sam Harrison*, Can You Make Money Selling Your Data?,* BBC (Sept. 20, 2018), https://www.bbc.com/worklife/article/20180921-can-you-make-money-selling-your-data [https://perma.cc/UD2P-36VL] (attempting to monetize personal data, author barely makes any money from the venture). Data valuation difficulties are further discussed in Section V.B.

122. *See* Lital Helman, *Pay for (Privacy) Performance: Holding Social Network Executives Accountable for Breaches in Data Privacy Protection*, 84 BROOK. L. REV. 523, 524 (2019); *see also* Kira M. Geary*, Section 230 of the Communications Decency Act, Product Liability, and A Proposal for Preventing Dating-App Harassment*, 125 PENN ST. L. REV. 501, 512 n.79 (2021) (quoting *Definition of: Big Tech*, PC MAG. (2019), https://bit.ly/3f3lmso (last visited Aug. 28, 2020)) (defining "Big Tech" as "major technology companies . . . which have inordinate influence").

of data.[123] This leads to an enormous amount of untaxed platform profits.[124] So while consumers *contribute* directly to platform profits, they receive nothing in return but ads that are specifically designed to target their preferences and get them to spend more.[125] Put simply, businesses not only lower costs by spending less energy obtaining relevant data but also cut costs by using cheap PII to create more effective advertisements. This cost cutting is further magnified on platforms like Amazon, where the platform itself functions both as a buyer and a seller in its market.[126]

Many argue that this "notice and choice" system is a fair trade and that users have essentially "consented" to paying with their data for certain services.[127] Yet, as discussed in Section II.B(1), consumers are prevented from making meaningful, informed choices.[128] Most platforms only offer access on a take-it-or-leave-it basis, and even then, users may *still* have their PII collected if they choose to "leave it."[129] Further, even if companies promise users not to collect or monetize their data, companies may do so anyway.[130] There is simply no meaningful user leverage within the current regime.

II. FAILURES OF CURRENT RESPONSES TO TARGETED DIGITAL ADVERTISING HARMS

The aforementioned problems need a solution.[131] Private law has attempted to address these harms, usually through tort, contract, and

123. *See* Elvy, *supra* note 64, at 1420–22. She notes that, even when consumers are paid for the rights to their personal data, the "largest obstacle to such a monetization method is the perceived value of a consumer's individual data, which may be worth significantly less than the vast quantities of aggregated data and customer lists companies hold." *Id.* at 1421. *See also* Harrison, *supra* note 121. *But see* Lucy Sherriff, *This App Enables You to Make Money Off Your Own Personal Data*, FORBES (Mar. 29, 2019, 3:48 PM), https://www.forbes.com/sites/lucysherriff/2019/03/29/this-app-enables-you-to-make-money-off-your-own-personal-data/#60f2c0d929f6 [https://perma.cc/N85K-VY6T] (discussing how certain consumers have used an app to successfully monetize some of their personal data).

124. *See* Thimmesch, *supra* note 1, at 150–55.

125. See Hu, *supra* note 16, at 312 (discussing the story of John, the fictitious consumer).

126. *See, e.g.*, Lauren Feiner, *Amazon Admits to Congress That it Uses 'Aggregated' Data from Third-Party Sellers to Come Up with Its Own Products*, CNBC (Nov. 19, 2019, 6:07 PM), https://www.cnbc.com/2019/11/19/amazon-uses-aggregated-data-from-sellers-to-build-its-own-products.html [https://perma.cc/V5W6-UD8P].

127. *See* Bamberger, *supra* note 65, at 336.

128. *See supra* Section II.B(1).

129. *See supra* text accompanying note 55.

130. *See* Chao, *supra* note 119, at 561–62; Austin-Spearman v. AARP, 119 F. Supp. 3d 1, 11–12 (D.D.C. 2015) (explaining "it is well established that not all promises rise to the level of binding contractual obligations," and "despite [plaintiff's] allegation that her membership fee was tendered . . . as consideration for AARP's promise to adhere to its Privacy Policy[,] . . . promises made in AARP's Privacy Policy were not a part of Austin–Spearman's binding AARP membership contract").

131. *See supra* Section II.

property law. Public law has made similar efforts in constitutional and regulatory law. Despite their best efforts, broad, pervasive harms remain.

A. Private Law

Private law deals with bimodal interactions regarding rights and obligations between private, nongovernmental entities and traditionally encompasses property, contracts, and tort law.[132] Private law's biggest failure in addressing data-driven harms is that its remedies are generally too narrow and individualized to address the disparate harms of PII collection and targeted advertising.[133] One plaintiff brings a case on her behalf—or even a class of similarly situated individuals—but rarely does private litigation achieve the type of relief needed to ameliorate gross societal harm.[134] Additionally, individual plaintiffs routinely encounter standing issues when trying to demonstrate a "concrete and particularized harm"[135] as privacy harms are notoriously difficult to pin down.[136] Furthermore, even if the plaintiff is able to prove a harm, their individual damages are likely to be so minimal as to make the cost of pursuing a lawsuit far outstrip any judicial remedy.[137] The structure of private law itself is a barrier to

132. Morton J. Horwitz, *The History of the Public/Private Law Distinction*, 130 U. PA. L. REV. 1423, 1424 (1982). Corporate law discussion, though substantially regulatory, is subsumed under contract law for the purposes of this Note.

133. *See* Ben-Shahar, *supra* note 18, at 106–07.

134. *See id.* at 106 (characterizing individual data harms as broader harms to the data "ecosystem").

135. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016), *as revised* (May 24, 2016). *See supra* discussion in Section II.B(1).

136. *See supra* Section II.B(2); Matthew S. DeLuca, Note, *The Hunt for Privacy Harms After* Spokeo, 86 FORDHAM L. REV. 2439, 2457 (2018).

137. *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Encourages Consumers to Opt for Free Credit Monitoring, as Part of Equifax Settlement (July 31, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-encourages-consumers-opt-free-credit-monitoring-part-equifax [https://perma.cc/NL2J-4NW3] (noting that so many consumers filed for damages that every consumer may not receive the $125 in damages they expected). *But see* Taylor Hatmaker, *Facebook Will Pay $650 Million to Settle Class Action Suit Centered on Illinois Privacy Law*, TECH CRUNCH (Mar. 1, 2021, 3:36 PM), https://techcrunch.com/2021/03/01/facebook-illinois-class-action-bipa/ [https://perma.cc/5P9Q-9GLU] (noting that a class action suit against Facebook for violating Illinois's Biometric Information Privacy Act garnered "at least $345 [per person] under the final settlement ruling in California federal court . . . ." for over one million residents).

addressing and remedying these harms; the structures of the three traditional private law classes detail further hindrances.

1. Contract Law

First, the data privacy regime in the United States is heavily contractual.[138] As discussed in Section II.B, this contractual "notice and choice" regime does not effectively stop pernicious data collection because it relies on coerced consent, bargaining power differentials, and few real alternative platforms.[139] Second, users often have no real way of finding out whether or not the company has violated their contract, especially in cases of data breaches or discriminatory use of PII, because they simply cannot peek behind the veil of Big Tech.[140] Also, if large platforms are found to violate the already generous contract terms of their sites, most suits for contractual violations go through mediation and arbitration, not the court system, creating a lack of meaningful precedent.[141] Finally, even if one looks to unjust enrichment,[142] contract law would likely impede this claim from going forward due to ostensible consent under the "notice and choice" regime.[143] Contract law offers little meaningful redress to the problem of large platform profits because it does not conceptualize profits as a problem

138. Bradyn Fairclough, *Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix It*, 42 J. CORP. L. 461, 466 (2016) (noting that data privacy is also tort-heavy).

139. *See supra* Section II.B.

140. *See* Bamberger, *supra* note 65, at 339.

141. *But see* Victoria Graham & Jake Holland*, Slew of Private Antitrust Suits Awaits Big Tech Under House Plan*, BLOOMBERG L. (Oct. 7, 2020, 3:05 PM), https://news.bloomberglaw.com/antitrust/slew-of-private-antitrust-suits-awaits-big-tech-under-house-plan [https://perma.cc/T32Z-V6UL] (discussing "a House Democratic proposal to dismantle big tech's market dominance in part by banning mandatory arbitration agreements").

142. Julia N. Mehlman, *If You Give A Mouse A Cookie, It's Going to Ask for Your Personally Identifiable Information: A Look at the Data-Collection Industry and a Proposal for Recognizing the Value of Consumer Information*, 81 BROOK. L. REV. 329, 354 (2015). "An unjust enrichment claim is a common theory of liability in contract law and is thought of as a quasi-contract claim. Courts have largely ignored unjust enrichment claims in relation to data collection and claims alleging that data collectors should compensate Internet users for their personal information." *Id.*

143. *But see* Chao, *supra* note 119.

where the parties "freely" contracted.[144] Rather, contract law sees large profits as the *point*.

2. Property Law

Property law provides an alternative model—perhaps pernicious data collection could be stopped if you "owned" your personal data.[145] Scholars have already proposed personal data ownership as a solution to privacy concerns[146] and used copyright law to claim ownership of certain PII with some success.[147] However, this approach is limiting. A copyrighted work must be both "independently created by the author" and have "some minimal level of creativity."[148] This means PII such as personal geolocation coordinates and "likes" are not copyrightable, but an artful selfie is. Even so, more property rights in PII would help curb pernicious data collection and help give more concrete value to what is "lost" in data breaches.[149] However, there is much concern that data as property would (1) be difficult to value[150] and (2) reifying data in this way may stymie free information exchanges[151] (but recent jurisprudence suggests that the second issue could be solved by treating data exchanges as bailments).[152] Even accepting the aforementioned benefits, increased property rights in PII would not stem the glut of untaxed platform profits. If anything, data ownership might help customers "see" the value of their data more, but companies would likely

144. Fairclough, *supra* note 138, at 472 ("Plaintiffs in these cases often claim the business breached their contract not to share their information only to find their claims are precluded because they have already signed away their privacy rights in a Terms of Use Agreement.").

145. *But see* Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1 (2018) (arguing against conceptualizing data as private property).

146. *See, e.g.*, Vera Bergelson, *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 383 (2003) (arguing "in order to protect privacy, individuals must secure control over their personal information by becoming its real owners").

147. *See, e.g.*, Kaitlan M. Folderauer, *Not All Is Fair (Use) in Love and War: Copyright Law and Revenge Porn*, 44 U. BALT. L. REV. 321, 322 (2015).

148. 77 AM. JUR. *Trials* 449 §§ 17, 137.5 (2000) (discussing copyright litigation).

149. This valuation would help with standing issues. *See supra* Sec.II.B(2).

150. *See* Thimmesch, *supra* note 1, at 179–81.

151. *See* Mark A. Lemley, *Private Property*, 52 STAN. L. REV. 1545, 1549 (2000).

152. *See* Carpenter v. United States, 138 S. Ct. 2206, 2269 (2018) (Gorsuch, J., dissenting) ("Just because you entrust your data . . . to a third party may not mean you lose any Fourth Amendment interest in its contents. . . . [E]-mail should be treated much like the traditional mail it has largely supplanted—as a bailment . . . .").

make overt what is implicit in platforms that offer ad-free subscriptions: your PII *is* the price you pay for access.[153]

3. Tort Law

Privacy claims in tort law are not novel.[154] William Prosser's influential traditional privacy torts[155] are as follows: intrusion upon seclusion (intrusion), appropriation of name or likeness (appropriation), public disclosure of private facts (disclosure), and false light.[156] This Note focuses on intrusion and appropriation. Intrusion gives rise to tort liability when one "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person."[157] Intrusion claims will usually fail as most platform users technically consent to platforms' data collection and "[e]ffective consent negates an intrusion upon seclusion claim."[158] Similarly, we are so used to platform data collection that any intrusion claim will likely fail to be "highly offensive to a reasonable person."[159] The second tort, appropriation, gives rise to liability when, without consent, one "appropriates to his own use or benefit the name or likeness of another."[160] Though a stronger argument around exactly *what* was consented to in the contract can be made under the "benefit" analysis, this will also likely fail for the same reasons as intrusion.[161] Even if it does not fail, recovery is so scant that plaintiffs are unlikely to actually bring suit under appropriation save for a class action.[162] Additionally, due to inherent platform/user power imbalances, it may be difficult for a user to know *when* their likeness or name has been appropriated—this is especially true in

153. *See* Magali Eben*, Market Definition and Free Online Services: The Prospect of Personal Data as Price*, 14 I/S: J.L. & POL'Y FOR INFO. SOC'Y 227, 229 (2018) (explaining that there is a "possibility of conceptualizing personal data as the price consumers pay for free online services").

154. *See* Lauren McCoy, *140 Characters or Less: Maintaining Privacy and Publicity in the Age of Social Networking*, 21 MARQ. SPORTS L. REV. 203, 206 (2010).

155. Peter W. Cooper, *The Right to Be Virtually Clothed*, 91 Wash. L. Rev. 817, 822 (2016).

156. RESTATEMENT (SECOND) OF TORTS § 652A (AM. L. INST. 1977).

157. *Id.* § 652B.

158. *See* Opperman v. Path, Inc., 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016). However, "consent is only effective if the person alleging harm consented 'to the particular conduct, or to substantially the same conduct' and if the alleged tortfeasor did not exceed the scope of that consent." *Id.* at 1072–73.

159. *Id.* at 1079–80. "Those customs and habits are very much in flux. . . . A judge should be cautious before substituting his or her judgment for that of the community." *Id.*

160. RESTATEMENT (SECOND) OF TORTS § 652C (AM. L. INST. 1977).

161. *See, e.g.*, *Opperman*, 205 F. Supp. 3d at 1072.

162. *See, e.g.*, Jesse Koehler, Fraley v. Facebook: *The Right of Publicity in Online Social Networks*, 28 BERKELEY TECH. L.J. 963, 964 (2013) (discussing the small individual recovery in a class action suit).

targeted advertising.[163] Even if you can prove that an advertiser was specifically targeting someone with your characteristics, it is very difficult to prove you were targeted by use of *your* PII—especially because courts struggle to define the term.[164] Though tort law has proven somewhat successful in dealing with data breach harms,[165] complex standing issues remain.[166] Still, other researchers have suggested public nuisance law could be a boon for corporate regulation.[167] While promising, the difficulty in proving tangible harm remains.

In the end, though private law offers creative solutions, its power-insensitive structure coupled with unique issues in tort, property, and contract law prevents it from fully ameliorating the unique harms of targeted advertising.

B. Public Law

Public law governs interactions between the State and private entities and traditionally encompasses constitutional, regulatory, and criminal law.[168] Public law's biggest failure thus far has not necessarily been its structure—the State certainly has broad, useful regulatory power—but rather its inability to effectively deter corporations from negative behavior due to agency underfunding in the face of multiple, powerful actors.[169]

1. Constitutional Law

Constitutional law poses several issues. The first, and most difficult to surmount, is the First Amendment commercial speech doctrine.[170] Limits on commercial speech (which includes advertising) are rare and must meet a

163. *See* Zuboff, *supra* note 13 (discussing "epistemic inequality," where consumers do not know about corporations, but corporations know about consumers).

164. Wendy Beylik, *Enjoying Your "Free" App? The First Circuit's Approach to an Outdated Law in* Yershov v. Gannett Satellite Information Network, Inc., 58 B.C. L. REV. E. SUPP. 60, 64 (2017) https://lawdigitalcommons.bc.edu/bclr/vol58/iss6/7 [https://perma.cc/3WVN-K4NS].

165. *See, e.g.*, Resnick v. AvMed, Inc., 693 F.3d 1317, 1327 (11th Cir. 2012).

166. *See supra* Section II.B(2).

167. See Ben-Shahar, *supra* note 18, for a general discussion of this theory.

168. *Private Law vs. Public Law*, DIFFEN, https://www.diffen.com/difference/Private_Law_vs_Public_Law [https://perma.cc/25DF-8EV8].

169. Charlie Osborne, *Lack of Funding Exposes US Federal Agencies to High Data Breach Risks*, ZERODAY (Feb. 22, 2018, 9:15 PM), https://www.zdnet.com/article/us-suffers-highest-data-breaches-of-government-agencies-worldwide/ [https://perma.cc/HQ93-MM7K]; *see also* Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1074–76 (2019) (noting that the FTC can only do so much, given its limited resources); Milan Babic, Eelke Heemskerk & Jan Fichtner, *Who is More Powerful—States or Corporations?*, CONVERSATION (July 10, 2018, 11:14 AM), https://theconversation.com/who-is-more-powerful-states-or-corporations-99616 [https://perma.cc/ZD46-8K7B].

170. *See infra* Section V.A.

high bar to be found constitutional.[171] Another common argument is that data itself is protected "speech" under the First Amendment, thus limiting government ability to constrain data transfers.[172] Professor Neil Richards, however, explains that this is a mistaken reading of the First Amendment,

> [T]his argument's consistency is a foolish consistency. Just because something is speech does not mean it is beyond regulation. . . . People also use words to hire assassins, engage in insider trading, sexually harass subordinates in the workplace, and verbally abuse their children. All of these activities are speech, but many of them are well outside the main concerns of the First Amendment. We need to protect some, but we need to regulate others.[173]

Furthermore, there are no Fourth Amendment issues, as proposed advertising regulations would take place in the commercial sector, not the government sector.[174] Similarly, though Fourteenth Amendment jurisprudence is relevant to privacy rights and data protection (the Supreme Court obliquely considered a right to data privacy in cases like *Whalen v. Roe*),[175] until there is an overt recognition of data privacy as a constitutional right,[176] there is little it can do to address targeted advertising.

2. Regulatory Law

Regulatory law offers the most promising and cohesive approach to privacy harms thus far. With Congress and multiple members of President Biden's administration discussing a federal omnibus privacy bill, 2021 may be the year a uniform, national statute regulating privacy rights is enacted.[177] However, until this bill becomes law, most federal privacy rights issues are

171. This issue merits extensive consideration and is separately addressed in Section V.A.

172. Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1524 (2015).

173. *Id.*

174. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).

175. 429 U.S. 589, 605–06 (1977).

176. *See Privacy's Constitutional Moment*, *supra* note 75.

177. *U.S. Cybersecurity and Data Privacy Outlook and Review–2021*, GIBSON DUNN (Jan. 28, 2021), https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2021/#_Toc62718885 [https://perma.cc/TB4Q-PWZV]. *See, e.g.*, Information Transparency & Personal Data Control Act, H.R. 1816, 117 Cong. (2021).

handled by individual agencies and a mishmash of broad statutes, each having unique strengths and weaknesses.

a. Antitrust Law

Some have argued stronger antitrust law enforcement will create a better privacy regime.[178] With the Department of Justice, the FTC, and a broad swath of state attorneys general filing antitrust suits against tech giants Facebook and Google, the future of their market domination is unknown.[179] While critics have decried these suits as unfair, breaking up these giants would, for better or worse, probably increase consumer *choice* by increasing competition.[180] Users may not so readily agree to Facebook's terms of service if another company provided a similar platform with stronger privacy rights.[181] However, while breaking up large tech companies would solve the monopolistic control of data and increase consumer choice, this approach still fails to stop smaller platforms from misusing data in the same way as large ones. Further, it fails to provide any clarity on the persistent issue of data breaches,[182] nor does it solve the issues of massive untaxed profits[183]—it just spreads the surplus around. Antitrust suits are a good starting point, but they cannot be the end.

b. The Federal Trade Commission

The FTC is the agency most responsible for regulating consumer protection law.[184] Given its long history of successful suits and censures of negative corporate behavior through its Federal Trade Commission Act Section 5(a) enforcement powers, the FTC is best suited to deal with consumer-protection-like harm.[185] In the past, the FTC has ordered binding consent decrees when it discovered companies were misusing consumer

178. *See, e.g.*, Cat Zakrzewski & Rachel Lerman, *Google Antitrust Case Centers on Consumer Choice and How Rivals Get Boxed Out*, WASH. POST (Oct. 20, 2020, 1:54 PM), https://www.washingtonpost.com/technology/2020/10/20/google-antitrust-suit-faq/ [https://perma.cc/4J9W-5SST].

179. Steven Pearlstein, *Facebook and Google Cases Are Our Last Chance to Save the Economy from Monopolization*, WASH. POST (Dec. 18, 2020, 7:00 AM), https://www.washingtonpost.com/business/2020/12/18/google-facebook-antitrust-lawsuit/ [https://perma.cc/8FVU-RXXQ].

180. *Id.*

181. *See generally* Zakrzewski & Lerman, *supra* note 178 (discussing user privacy concerns).

182. *See supra* Section II.B(2).

183. *See infra* Section III.B(3).

184. *See* Skelton, *supra* note 109, at 306.

185. *Id.* Consumer protection harms include harms arising from "unfair, deceptive and fraudulent business practices," including scams, fraud, and robocalls. *Bureau of Consumer Protection*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection [https://perma.cc/JVF5-SHQ4].

data[186] and has taken companies with inadequate security practices to court for data breach harms.[187]

However, there are several problems with the FTC's current regulatory approach. First, while the FTC might be able to disincentivize companies from participating in pernicious data privacy violations, the FTC enforces statutory law and community norms.[188] Aggressive data collection and targeted digital advertising are the norm as of now, and until these practices are made illegal, or the FTC decides that they are "deceptive or unfair," there is no meaningful way to address these harms. Second, though the FTC is exceptionally good at prosecuting data breaches, Section 5 contains no private right of action.[189] Given that it is a large agency with limited resources, the FTC must choose to go after larger harmful actors at the expense of passing up smaller bad actors in the industry.[190] This creates an issue wherein someone may have been harmed by a data breach but the FTC does not act, its "failure to move against violators" potentially resulting from "resource limitations and not from exercise of discretion."[191] This leaves the victim with recourse only in tort law, which, as discussed, has onerous standing issues.[192] Third, the FTC has injunctive power and the power to levy fines, but rarely do these hefty fines amount to anything more than a "slap on the wrist."[193] Abusing data is so profitable that even in light

186. *See, e.g.*, Stuart L. Pardau & Blake Edwards, *The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity*, 12 J. BUS. & TECH. L. 227, 238 (2017) (explaining that the "FTC has since taken the lead in setting cybersecurity standards, developing something like a body of common law with its vast collection of complaints, privacy guides, and consent decrees"). The article provides an overview of the FTC's role in prosecuting data security issues in the Big Tech sphere. *Id.* at 241–43.

187. *See, e.g.*, Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 259 (3d Cir. 2015).

188. *See* 54A AM. JUR. 2d *Monopolies and Restraints of Trade* § 1132 (2021) ("Congress believed that unfair competition could best be prevented through the action of an administrative body of practical people who could apply the congressional standard to particular business situations so as to eradicate evils with the least risk of interfering with legitimate business operations."); *See also* David L. Belt, *The Standard for Determining "Unfair Acts or Practices" Under State Unfair Trade Practices Acts*, 80 CONN. BAR J. 247, 255 (2006).

189. *See* Edoho-Eket v. Wayfair.com, No. 17-6509, 2019 WL 2524366, at *2 (6th Cir. Jan. 23, 2019) (citing Fed. Trade Comm'n v. Owens-Corning Fiberglass Corp., 853 F.2d 458, 464 (6th Cir. 1988)) (holding "Section 5 of the FTCA does not provide a private right of action").

190. Comment, *Implied Consumer Remedy Under FTC Trade Regulation Rule—Coup De Grâce Dealt Holder in Due Course?*, 125 U. PA. L. REV. 876, 902 (1977).

191. *Id.*

192. *See supra* Sec. III.A(3).

193. Jonathan Schieber, *Facebook Reportedly Gets a $5 Billion Slap on the Wrist from the FTC*, TECHCRUNCH (July 12, 2019, 2:10 PM), https://techcrunch.com/2019/07/12/ftc-gives-facebook-5-billion-wrist-slap/ [https://perma.cc/M8PG-5PU8]. *See also* Anna B. Naydonov, *SCOTUS: FTC Has No Authority to Obtain Monetary Relief Under Section 13(b) of the FTC Act*, NAT'L L.R. (May 14, 2021), https://www.natlawreview.com/article/scotus-ftc-has-no-authority-to-obtain-monetary-relief-under-section-13b-ftc-act. Naydonov explains in the recent Supreme Court case, *AMG Cap. Mgmt., LLC v. Fed. Trade Comm'n*, 141 S. Ct. 1341, 1343 (2021), the Court "held that Section 13(b) of the Federal Trade Commission Act does not give the Commission authority to bypass administrative proceedings

of a million-dollar fine, corporations will take the fine and continue with their bad practices and big profits.[194] Finally, the FTC does not adjust for the inherent *economic* imbalance between platforms and users—unless a platform engages in "unfair or deceptive" acts, there is no actionable issue.[195] Unless the FTC updates its "unfair or deceptive" practices to include broad, systemic data inequity and privacy harms, the FTC will not be able to resolve this issue.

c. Data Protection Law

There *are* statutes in the United States that protect PII, but they are sectoral statutes,[196] not general ones; thus, they are unable to address broad harms across multiple mediums. The Health Insurance Portability and Accountability Act (HIPAA), for example, strongly protects personal *health* information, but only if it is held by a "covered entity."[197] For example, while your doctor cannot monetize your personal health data, your Apple watch that collects information about your daily steps and average fitness level *can*.[198] A broad national HIPAA-like data protection law would certainly restrict data collection and thus almost certainly make targeted ads impossible. It would also be opposed by businesses, especially smaller ones that can use online targeted advertising to cut costs.[199] While this might solve the pernicious data collection, data breach, and economic imbalance issues, it would likely be too restrictive to allow businesses to engage in online commerce and would likely sacrifice the positives of targeted

and seek equitable monetary relief directly from the federal courts." *Id.* The FTC's acting chairwoman at the time urged Congress to remedy this decision, saying administrative proceedings and other avenues, while useful "will [not] come close to protecting consumers and incentivizing compliance as much as our lost 13(b) authority." *Id.*

194. *See* Darlene. R. Wong, *Stigma: A More Efficient Alternative to Fines in Deterring Corporate Misconduct*, 3 CAL. CRIM. L. REV. 3, ¶ 56 (2000) (discussing corporate cost internalization of fines and proposing a legal "stigma" solution).

195. *See* 15 U.S.C. § 45(a)(1).

196. *See Privacy's Constitutional Moment*, *supra* note 75, at 1704.

197. *Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html [https://perma.cc/5VE5-AWKR].

198. Reinhardt Krause, *How Apple Privacy Policy Could Unlock A Big Health Care Market*, INVESTORS (June 28, 2019, 1:10 PM), https://www.investors.com/news/technology/apple-privacy-policy-data-privacy-healthcare-market/ [https://perma.cc/HMV2-ZWWV].

199. Steve Strauss, *Small Biz Owners, Take Advantage of Targeted Marketing to Reach Your Audience*, USA TODAY (Oct. 28, 2020, 2:28 PM), https://www.usatoday.com/story/money/columnist/2020/10/28/how-does-digital-marketing-work-small-businesses/3752350001/ [https://perma.cc/MB7A-3WQ3].

advertising along with the negatives. However, state-level data protection laws provide less restrictive alternatives.

3. State Omnibus Privacy Laws: The CCPA

The most well-known state-based response to modern privacy harms in the United States is the California Consumer Privacy Act of 2018 (CCPA).[200] This Note will use the CCPA as an example of model state legislation, as it is widely considered to be the most comprehensive and cutting-edge privacy regulation in the United States.[201] The CCPA is centered around several basic privacy rights: 1) the right of the user to know which PII is being collected and to access said data, 2) the right to request deletion of said data, 3) the right to know to whom the data is being sold, 4) the right to opt out of said data sales, and 5) a limited right to equal services and pricing if one opts out of data collection entirely.[202] Though these CCPA rights are robust and useful, companies like Facebook and Google still exploit a major loophole. As discussed in the introduction, Facebook has argued it does not "sell" user data—it merely sells targeted advertisements to third parties.[203] So, while Facebook does not directly hand over your status as say, a new mother who lives in St. Louis in the 22% tax bracket, a third party can tell Facebook, "I would like to advertise these diapers to new mothers in the 22% tax bracket who live in St. Louis," and Facebook will "place" those ads for them. There is technically no "sale" of data, though large troves of consumer data are still being used and advertisers can still target users on a highly individualized basis for massive profits.[204] Further, the CCPA again relies heavily on the preexisting "notice and choice" regime, which has been ineffective in encouraging companies to behave

200. *See* David Alpert, Note, *Beyond Request-and-Respond: Why Data Access Will Be Insufficient to Tame Big Tech*, 120 COLUM. L. REV. 1215, 1215 (2020) (noting the CCPA is the "first-of-its-kind" in the United States); s*ee also* Alexander H. Southwell, Ryan T. Bergsieker, Cassandra L. Gaedt-Sheckter, Frances A. Waldmann & Lisa V. Zivkovic, *Virginia Passes Comprehensive Privacy Law*, GIBSON DUNN (Mar. 8, 2021), https://www.gibsondunn.com/wp-content/uploads/2021/03/virginia-passes-comprehensive-privacy-law.pdf [https://perma.cc/4EFW-BHVJ] (explaining "Governor Ralph Northam signed the Virginia Consumer Data Protection Act ('VCDPA') into law" on March 2, 2021 and that "Virginia is only the second state to enact a comprehensive state privacy law, . . . yet its substance draws from both . . . the California Consumer Privacy Act ('CCPA'), and the newly enacted California Privacy Rights and Enforcement Act ('CPRA')").

201. *See* Elaine F. Harwell, *What Businesses Need to Know About the California Consumer Privacy Act*, AM. BAR ASSOC. (Oct. 7, 2019), https://www.americanbar.org/groups/business_law/publications/blt/2019/10/ca-consumer-privacy/ [https://perma.cc/H2N3-4WFD].

202. *See* Diane Y. Byun, *Privacy or Protection: The Catch-22 of the CCPA*, 32 LOY. CONSUMER L. REV. 246, 251 (2020).

203. *See supra* note 2 and accompanying text.

204. *See, supra* note 7 and accompanying text.

"better" when they collect data.[205] The CCPA also fails to account for the inherent producer/consumer power imbalance.[206]

IV. PROPOSAL

The vast majority of user data collection goes to fuel advertising sales, and it is unlikely the aforementioned options will stop this trend.[207] Private law's structure, at least currently, cannot address these new harms.[208] Public law is underfunded and outgunned by large tech corporations.[209] Finally, for better or worse, many consumers[210] still use and enjoy ostensibly free social media platforms even if they are troubled by the companies' business practices.[211] Limiting abusive corporate data practices is helpful, but disallowing for targeted advertising entirely may push the cost onto consumers, leading to a "pay for privacy" plan.[212]

This is why taxation is a powerful tool. First, taxes can address inevitable, pervasive *public* harms caused by individualized private actions.[213] While not being entirely able to *halt* pernicious PII collection practices, a tax would make sure each sale of a targeted advertisement created by the use of PII would rack up a small "fine." This would be more effective than nuisance law[214] or piecemeal FTC enforcement.[215] Unlike nuisance law, there is no need to prove a harm,[216] and unlike the FTC's Section 5 enforcement paradigm, there is no need to investigate and prioritize targeting large, bad actors.[217] The action in and of itself justifies taxation, so taxes can be levied without looking into harm or investigating "unfair or deceptive" practices.[218] Second, taxes provide a stream of revenue, so underfunded agencies[219] would have a more reliable revenue

205. *See supra* Section II.B(1).
206. *See supra* Section II.B(3).
207. *See supra* Section III.
208. *See supra* Section III.A.
209. *See supra* Section III.B.
210. *See* Esteban Ortiz-Ospina, *The Rise of Social Media*, OUR WORLD IN DATA (Sept. 18, 2019), https://ourworldindata.org/rise-of-social-media [https://perma.cc/4RN6-RQXV].
211. Casey Newton, *Facebook's Trust Problem Isn't About Being Understood*, VERGE (Jan. 31, 2020, 6:00 AM), https://www.theverge.com/interface/2020/1/31/21115104/facebook-mark-zuckerberg-liked-understood-trust [https://perma.cc/YT9M-ETCM].
212. *See supra* text accompanying note 82.
213. *See* Ben-Shahar, *supra* note 18, at 110 (explaining that public harms arise from individual data usage).
214. *See supra* Section III.A(3).
215. *See supra* Section III.B(2)(b).
216. *See* Ben-Shahar, *supra* note 18, at 125 (discussing harms and theories of causation under tort law).
217. *See supra* Section III.B(2)(b).
218. *See supra* text accompanying note 195.
219. *See* Osborne, *supra* note 169 (discussing the FTC's lack of funds).

source to fund enforcement. Additionally, these taxes could potentially provide a monetary safety net for individuals harmed by data breaches, providing backup funds if companies cannot adequately compensate all individuals harmed.[220] Third, while not fully correcting the platform/user economic imbalance, a tax on digital targeted advertising that is created by use of PII would still force companies to "pay" for some of the user data they monetize.[221] A tax on PII-created digital targeted advertising would serve to both admonish negative private actions and provide a safety net for addressing disparate, public data harms without banning the practice altogether. This tax would make overt the tradeoff we, as a society, are willing to make for platform access as weighed against our privacy concerns.

A. The First Proposal: Elimination of the Advertising Deduction for Ads Created by Use of PII

The corporate income tax[222] is one of the more widely supported taxes in the United States.[223] Under this tax, corporate income is taxed by the federal government at a 21% rate,[224] minus allowable deductions.[225] These allowable deductions include certain "advertising and other selling expenses"[226] under the IRC's "business expenses" provision.[227] The policy rationale behind this is simple: the government does not want to tax the *cost* of doing business, it wants only to tax *profit*, thereby preserving its longstanding policy of economic neutrality.[228]

The denial of a deduction for targeted ads created by use of PII would not only help recover lost consumer market input and disincentivize, however slightly, the use of targeted ads, but would also be relatively easy to implement, at least from a drafting standpoint. First, Congress would

220. This would assist with data breach recovery. *See supra* Section III.B(2); text accompanying note 137.

221. *See supra* Section II.B(3).

222. I.R.C. § 11 (West).

223. *See* Isabel V. Sawhill & Christopher Pulliam, *Americans Want the Wealthy and Corporations to Pay More Taxes, but Are Elected Officials Listening?*, BROOKINGS INST. (Mar. 14, 2019), https://www.brookings.edu/blog/up-front/2019/03/14/americans-want-the-wealthy-and-corporations-to-pay-more-taxes-but-are-elected-officials-listening/ [https://perma.cc/2PZM-8T8M].

224. I.R.C. § 11(b) (West). State and local taxes generally increase this rate. *See* Kyle Pomerleau, *The United States' Corporate Income Tax Rate is Now More in Line with Those Levied by Other Major Nations*, TAX FOUND. (Feb. 12, 2018), https://taxfoundation.org/us-corporate-income-tax-more-competitive/ [https://perma.cc/W29M-PPW3].

225. I.R.C. § 1.161-1 (West).

226. I.R.C. § 1.162-1(a) (West).

227. I.R.C. § 162 (West).

228. *See, e.g.*, Jason Furman, *The Concept of Neutrality in Tax Policy*, BROOKINGS INST.: TESTIMONY (Apr. 15, 2008), https://www.brookings.edu/testimonies/the-concept-of-neutrality-in-tax-policy/ [https://perma.cc/77UF-6VTQ].

need to pass an amendment to the IRC, similar to I.R.C. § 162(e), denying a deduction for targeted advertising that uses PII.[229] Then, Congress would need to clearly define both targeted advertising and PII, potentially using the CCPA for reference.[230] In the end, this removal does not *add* any significant burden, it merely reduces the ability of the company to write off such expenses.

This removal would first allow the government to recoup some of the platform user's lost PII value, likely without passing on any major downstream costs to the platform user, as opposed to a direct tax on data collection,[231] which will be discussed in Section V.[232] Second, this is not a tax, so no discrete transactional value needs to be calculated or a new rate discussed—the advertiser simply loses the ability to deduct an expense. Third, once norms have shifted and the advertisers understand that certain targeted ads are not tax deductible, they might be more selective about their use of such ads. Fourth, and most importantly, this would encourage platforms that generate much of their revenue from monetizing PII-generated ads and ad placements to begin offering ads that use *deidentified* data, so as not to lose advertiser business. Though the IRS may need to employ extra effort to monitor compliance, the question of whether a deduction should be allowed or denied is simple: was the ad "placed" or "sold" using PII or not? If it was, no deduction is allowed. Further, additional costs the IRS incurs in enforcing this provision could also be financed by proceeds from the tax itself, and excess tax proceeds could be directed towards the FTC or other regulatory agencies that specialize in monitoring consumer protection and data protection. Though there is certainly likely to be debate in defining precisely what constitutes a PII-created targeted advertisement, the courts are certainly capable of handling any issues that might arise.

B. The Second Proposal: An Excise Tax on Advertising that Uses PII

While the removal of a targeted advertising expense deduction disincentivizes the *purchase* of ads, or the demand side of the transaction, there should be a similar tax mechanism on the *creation* of such ads, or the supply side of the transaction.[233] An excise tax on the sale of digital targeted

229. I.R.C. § 162 (West).

230. *See supra* text accompanying note 1.

231. *See* Thimmesch, *supra* note 1, at 178–79 (explaining "that the imposition of tax on individuals' personal-data gains would be particularly problematic because such a tax would likely . . . disproportionately impact[] lower-income taxpayers" as opposed to wealthier internet users).

232. *See infra* Section V.B.

233. *See* Amy Sinden, *The Tragedy of the Commons and the Myth of a Private Property Solution*, 78 U. COLO. L. REV. 533, 541 (2007) (explaining supply and demand curves).

ads created by use of PII will then be an appropriate measure for addressing the generalized harm that pernicious data collection practices invite. However, this is a complicated proposal. First, there are many potential ways to impose such digital tax, each with strengths and weaknesses.[234] This Note advocates for an excise tax, but acknowledges that there are several viable alternatives. Second, the tax rate must be fixed at a rate high enough to discourage aggressive, dangerous data collection but not so high as to shift major downstream costs onto small business and platform users.[235]

There are two main ways to impose excise taxes in the U.S.—ad valorem taxes or per unit taxes.[236] A tax is ad valorem when it is "applied as a percentage of the value of the product, either based on the manufacturer's, wholesale, or retail price."[237] For example, the IRS imposes an ad valorem excise tax on the use of tanning bed, taxing "any indoor tanning **service [at] a . . . [rate of] equal to 10 percent of the amount paid for such service** (determined without regard to this section)"; [238] thus, the tax applies to the provider-set price. However, per unit taxes "[are] applied per individual unit produced, purchased, or sold."[239] So one portion of gasoline tax, for example, is applied at "18.3 cents per gallon."[240]

This Note suggests the use of an ad valorem excise tax. To begin, ad valorem taxes are better suited to keep up with inflation, as "they are applied based on the *price* of commodity or activity rather than the quantity consumed or produced"; thus, an ad valorem tax would be best suited to keep pace with the rapidly-growing targeted digital ad industry.[241] Further, though it is likely companies will still cry foul over an excise tax in general, an ad valorem tax set up as a percentage of a company-set price may give the company more control in determining its precise tax liability. Finally, ad valorem taxes "can also be more progressive than per-unit rates," particularly when "demand increases more than proportionally as income

234. *See* Fuchs, *supra* note 24, at 16 (reviewing policy options for online ad taxes). This report provides more information on alternative tax structures, which are beyond the purview of this Note.

235. *See* Walczak, *supra* note 12. When discussing Maryland's new ad tax, Walczak explains that not only would a high tax disproportionately harm small businesses that purchase such ads, but "to the extent that the tax falls on . . . businesses, not only will much of the cost be imposed in Maryland, but some of it also will be passed along to consumers themselves." *Id*.

236. SEAN LOWRY, CONG. RSCH. SERV., FEDERAL EXCISE TAXES: AN INTRODUCTION AND GENERAL ANALYSIS 5 (2013).

237. *Id.*

238. I.R.C. § 5000B(a) (West) (emphasis added).

239. LOWRY, *supra* note 236, at 5.

240. I.R.C. § 4081(a)(2)(A)(i).

241. LOWRY, *supra* note 236, at 5; *see also Digital Advertising Spending Worldwide 2019-2024*, STATISTA (May 28, 2021), https://www.statista.com/statistics/237974/online-advertising-spending-worldwide/ [https://perma.cc/ZUA8-WRBY] (noting that "[d]igital advertising spending worldwide . . . stood at an estimated 378 billion U.S. dollars in 2020. . . . [And is expected to] increase in the coming years, reaching a total of 646 billion U.S. dollars by 2024").

rises."[242] Though small businesses buy advertisements, and ad valorem taxes run the risk of becoming regressive if the taxed product is purchased at a greater rate by those in the lower income brackets,[243] the vast majority of ad purchases are carried out by large companies.[244] To be fair, an ad valorem tax runs the risk of being ineffective (as the company is free to adjust its prices so as to avoid a major tax), but it is still preferable to a per unit tax, which will likely be more regressive and fail to keep up with inflation.

Deciding the rate is always a difficult question: federal excise tax rates hover around 7–12%.[245] Perhaps the most sensible approach would mimic environmental excise taxes, specifically carbon taxes,[246] since targeted advertising sales deal with similar risks to the digital environment. However, seeing as carbon taxes are per unit, it may be difficult to calculate an appropriate tax rate.[247] Additionally, Maryland recently passed a digital advertising sales tax with rates "up to 10[%]"[248] and was met with notable blowback.[249] Given the obvious resistance to a tax rate this high, Congress

242. LOWRY, *supra* note 236, at 5–6.

243. *Id*.

244. Ivan De Luce, *10 Companies That Spent More Than $1 Billion in Ads so You'd Buy Their Products*, BUS. INSIDER (Oct. 4, 2019, 9:20 AM), https://www.businessinsider.com/10-biggest-advertising-spenders-in-the-us-2015-7 [https://perma.cc/VT5H-S9LC]. Every company mentioned in this article was a large corporation. *Id*. Further, the largest U.S. corporations, on average, spend two percent of their revenue on advertising, whereas small businesses, on average, only spend one percent of their budgets. *Compare* Patricia Laya, *Do You Pay Enough for Advertising? One Big Corporation Spent A Jaw-Dropping $4.2 Billion Last Year*, BUS. INSIDER (June 6, 2011, 12:57 PM), https://www.businessinsider.com/corporations-ad-spending-2011-6#hewlett-packard-spent-1-billion-on-advertising-1 [https://perma.cc/8HRC-FSPZ], *with* Shawn Hessinger*, How Much Do Small Businesses Spend on Advertising and Marketing?*, SMALL BUS. TRENDS (Jan. 22, 2021), https://smallbiztrends.com/2018/04/much-small-businesses-spend-on-advertising-marketing.html [https://perma.cc/PY79-TEMY] (noting, however, that certain industries spend more on advertising than others).

245. *See* Julia Kagan, *Excise Tax*, INVESTOPEDIA (Apr 28, 2020), https://www.investopedia.com/terms/e/excisetax.asp [https://perma.cc/2LBH-S8EQ].

246. *See What Is a Carbon Tax?*, TAX POL'Y CTR. (May 2020), https://www.taxpolicycenter.org/briefing-book/what-carbon-tax [https://perma.cc/H84A-EZMP]; *but see* Ben-Shahar, *supra* note 18, at 138–40.

247. *See id.*

248. *See* Walczak, *supra* note 12.

249. *See* Sam McQuillan, *Maryland's Digital Ad Tax Guidance Coming This Week (1)*, BLOOMBERG L. (June 3, 2021, 3:10 PM), https://www.bloomberglaw.com/bloomberglawnews/daily-tax-report/X1669GSG000000?bna_news_filter=daily-tax-report [https://perma.cc/2Y3N-CXRR] (noting "[s]everal giant tech companies . . . are suing over the law . . ."); Michael J. Semes & Jared Walczak, *Maryland's Digital Advertising Tax Is Unworkably Vague*, Tax Foundation (Feb. 10, 2021), https://taxfoundation.org/maryland-digital-advertising-tax-vague/ [https://perma.cc/WE9Q-QWA5] (noting the law's constitutionality has been called into question, and that the vaguely worded statute opens the door to double taxation).

should aim for a low rate, perhaps even around 2%, as even a *slight* tax could substantially increase revenue.

Implementation of this tax will be more difficult than merely closing the targeted advertising deduction. First, companies will likely argue that *their* advertising does not fit the definition of PII-created advertising, meaning the early years of implementation may be wrapped up in litigation interpreting the tax itself. Second, corporations are no strangers to "creative financial techniques"[250] meant to lighten their tax burden, so this will require much time, effort, and diligence from the IRS and related agencies. Third, tech corporations are not tied to a particular location the same way traditional corporations are, and it is therefore likely that they may amend their articles and incorporate in overseas, low-tax or no-tax countries to avoid paying the tax.[251]

However, simply because implementation is difficult does not mean it is impossible. Big Tech companies, many of which rely on third party advertising to generate profits, regularly rake in billions of dollars each year,[252] and even a collecting a small portion of that would go a long way in funding IRS enforcement and other regulatory agencies.

V. MAJOR ISSUES

A. Sorrell *and the Commercial Speech Doctrine*

One of the biggest hurdles the tax will face is likely the commercial speech doctrine. This doctrine holds that commercial speech, or speech involving economic activity, can be more freely regulated by statute than can First Amendment protected speech.[253] For example, Congress can regulate how a company labels its shampoo bottles but not a reviewer's personal opinions about the shampoo. The Supreme Court evaluates

250. Eduardo Porter, *The Trouble With Taxing Corporations*, N.Y. TIMES (May 28, 2013), https://www.nytimes.com/2013/05/29/business/the-trouble-with-taxing-corporations.html [https://perma.cc/3L6C-ZBRL].

251. *Id. See also* David J. Brennan, Jr., *Avoiding the Sales Tax Economic Nexus Train Wreck*, J. ACCOUNTANCY (Sept. 1, 2020), https://www.journalofaccountancy.com/issues/2020/sep/sales-tax-economic-nexus-rules.html (discussing which states have more or less favorable economic nexus laws in the wake of South Dakota v. Wayfair, Inc., 138 S. Ct. 2080 (2018)).

252. *See* Elaine S. Povich, *Taxing Internet Ads Could Raise Lots of Money, but Doubts Persist*, PEW RSCH. CTR. (Feb. 25, 2020), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/02/25/taxing-internet-ads-could-raise-lots-of-money-but-doubts-persist [https://perma.cc/DNU6-7T2R].

253. Pittsburgh Press Co. v. Pittsburgh Comm'n on Human Rels., 413 U.S. 379, 384–85 (1973) (explaining the history of the commercial speech doctrine).

commercial speech restrictions using the intermediate scrutiny standard[254] and the *Central Hudson* test:[255]

> Courts must determine whether: (1) the speech concerns lawful activity and is not misleading; (2) the asserted governmental interest is substantial; (3) the regulation directly advances the governmental interest asserted; and (4) "whether it is not more extensive than is necessary to serve that interest."[256]

To further complicate matters, courts also recognized that *strict* scrutiny should generally—but not always—be applied when evaluating commercial speech subject to speaker and/or content-based restrictions.[257] This confusing multiplicity of doctrines recently clashed with the world of data in *Sorrell v. IMS Health Inc.*,[258] where the Supreme Court briefly considered classifying certain data as speech.[259]

Sorrell concerned a Vermont statute that prohibited "pharmacies and other regulated entities from selling or disseminating prescriber-identifying information for marketing."[260] Pharmacies and data mining agencies in Vermont argued that this regulation impermissibly burdened their First Amendment free speech right, while the State argued that the statute only regulated commercial speech and was therefore constitutional.[261] Justice Kennedy, writing for the majority, found that "[s]peech in aid of pharmaceutical marketing . . . is a form of expression protected by the Free Speech Clause of the First Amendment,"[262] and even

254. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 573 (Blackmun, J., concurring); *see also* Greater Phila. Chamber of Com. v. City of Philadelphia, 949 F.3d 116, 138 (3d Cir. 2020).

255. Thompson v. W. States Med. Ctr., 535 U.S. 357, 367 (2002).

256. *Greater Phila. Chamber of Com.*, 949 F.3d at 138 (quoting *Cent. Hudson*, 447 U.S. at 566).

257. *Id.* at 139. The Court held that "it may be appropriate to apply strict scrutiny to a restriction on commercial speech that is viewpoint-based" and "the rule that content-based speech restrictions are subject to strict scrutiny is 'not absolute' and is inapplicable when the restriction does not '"raise[ ] the specter that the Government may effectively drive certain ideas or viewpoints from the marketplace."' *Id.* (quoting R.A.V. v. City of St. Paul, Minnesota, 505 U.S. 377, 387–88 (1992)).

258. 564 U.S. 552 (2011).

259. *Id.* at 570. The Court explained that it "has held that the creation and dissemination of information are speech within the meaning of the First Amendment." *Id.* It further noted that "[f]acts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs," and that there was "a strong argument that prescriber-identifying information is speech for First Amendment purposes." *Id.* However, it declined to answer whether that information was speech in this case. *Id.* at 571. *But see Privacy's Constitutional Moment*, *supra* note 75, at 1731. The authors note that they worry "about spurious First Amendment objections derailing policy discussions and being used as further ammunition to weaken any privacy rules introduced before Congress. Arguments that 'data is speech' and thus data protection rules are censorship have rhetorical appeal*, even though they break down completely under serious analysis*." *Id.* (emphasis added).

260. *Sorrell*, 564 U.S. at 562.

261. *Id.* at 557.

262. *Id.*

though the Vermont statute purported to merely regulate commercial speech, it impermissibly regulated "certain content and . . . particular speakers."[263] That is to say, it regulated pharmacy companies and "data miners"[264] and their right to convey certain kinds of information. This meant that the statute needed to be evaluated under "heightened judicial scrutiny" in lieu of intermediate scrutiny.[265] Kennedy then found that the Vermont statute failed to meet this heightened standard because (1) the statute imposed a content-based burden on pharmaceutical companies seeking to "speak" to doctors[266] and (2) this burden was unjustified as it was not the least restrictive means of protecting patients (Vermont's stated policy objective).[267]

This is problematic because, though the Court's opinion was muddled, *Sorrell* might be interpreted as regulating data, and the transfer of data, as First Amendment protected speech.[268] This would make restriction on data "constitutionally suspect,"[269] and some scholars have suggested *any* statute aimed at regulating data flows or privacy protection would be dead on arrival.[270] However, other scholars insist that this doomsday interpretation of *Sorrell* is alarmist and inaccurate and that the First Amendment will not end data regulation—rather, "regulation of the commercial trade in personal data will be consistent with the First Amendment, at least most of the time."[271] While inconclusive, *Sorrell* certainly still presents a troubling hurdle to overcome.

To begin, insofar as the first proposal goes, removing a deduction is *not* a tax. Congress has repeatedly disallowed deductions for certain expenses, most noticeably forbidding any deductions for "certain lobbying and political expen[ses]," [272] making political ads one of the few categories of advertising that is *not* tax-deductible. Therefore, the first proposal will likely raise no constitutional issues.

The second proposal is more troubling. It will certainly burden speech, but not in the same way as was done in *Sorrell*[273]—it will not ban any "speech" outright, merely burden it through taxation. This is potentially a

263. *Id.* at 567.
264. *Id.* at 558–59.
265. *Id.* at 557.
266. *Id.* at 568.
267. *Id.* at 592 (Breyer, J., dissenting) (critiquing the majority for "inviting courts to scrutinize whether a State's legitimate regulatory interests can be achieved in less restrictive ways whenever they touch (even indirectly) upon commercial speech").
268. *See* Richards, *supra* note 172, at 1521–22.
269. *Id.* at 1522.
270. *See, e.g.*, Ashutosh Bhagwat, Sorrell v. IMS Health*: Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 868 (2012).
271. *See* Richards, *supra* note 172, at 1505.
272. I.R.C. § 162(e) (West).
273. *See supra* text accompanying notes 258–65.

mark in its favor. Secondly, this tax could pass the *Central Hudson* speech test.[274] Under the test, (1) the speech concerns lawful activity and is not misleading, (2) the asserted government interest in protection user privacy and consumer rights is arguably quite substantial, (3) this regulation directly advances the government interest in recognizing and "reining in" the harm of targeted digital advertising, and (4) it is a narrowly tailored statute that will serve *only* the interest in regulating digital advertising harms that use PII—if companies want to avoid this, they can use deidentified data. Finally, though it *could* be argued this statute regulates both content and viewpoint, it is narrowly tailored, and corporations can easily employ *nontargeted* digital advertising as a replacement, easily opting out of the tax. In conclusion, there is unlikely a substantial First Amendment freedom of speech threat to the third-party advertising tax.

B. Why Not a Tax on Data Collection Itself?

Several scholars, like Professors Ben-Shahar and Thimmesch, have toyed with the idea of imposing a tax on PII transactions.[275] Essentially, in lieu of taxing targeted digital advertisements, PII *transactions* between platform users and corporations would be taxed, likely at the time of data collection.[276] Under this framework, a corporation would pay a tax each time it collected user PII. For example, if a website collected information about your birthday when you created an account, a tax would be levied on that transaction. The taxation of this transaction could be formatted any number of ways, but the goal would likely be—as with a digital advertising tax—balancing the positive and negative effects of massive PII aggregation.[277]

If one accepts the premise that data collection generates inescapable negative externalities, this would be a great idea. However, due to the nature of data, such a tax would be difficult to impose because, among other issues, (1) it is hard to "value" each individual's personal data at the point of collection, (2) this tax would impose downstream costs, and (3) collecting the tax would be an administrative nightmare.[278] The first issue arises for several reasons. First, "[t]here have never been real cash markets for

274. *See supra* text accompanying note 255–51.

275. *See generally* Thimmesch, *supra* note 1, *and* Ben-Shahar, *supra* note 18, at 139–42.

276. *See* Ben-Shahar, *supra* note 18, at 139 (Ben-Shahar suggests for this to be formatted like the existing carbon tax).

277. *Id.* at 139–40.

278. Masur & Posner, *supra* note 274, at 178; *see also* Thimmesch, *supra* note 1, at 173–81. Thimmesch discusses five major issues with imposing a personal data transfer tax: "(1) seemingly insurmountable valuation problems; (2) the difficulties of line drawing; (3) the distribution of the resulting tax burden; (4) the anonymous Internet; and (5) the lack of political will." *Id.* at 174. However, this Note focuses on three.

personal data," and even if such markets existed, data transaction are *continuous*, thus, it is hard to pinpoint when, if ever, a PII transaction is complete.[279] Contrarily, advertisement sales *do* have concrete, cash values, and are discrete, time-bound transactions. For the second issue, if every user's data costs $5 to collect, it seems reasonable to believe some platforms would either begin charging a service fee or institute a pay-for-privacy plan, both of which would disproportionately harm low income users.[280] An ad valorem excise tax on advertisements alone, contrarily, would minimize this harm.[281] Additionally, it would be obscenely difficult for the IRS to oversee every single data collection transaction.[282] An ad valorem tax on advertising transactions again addresses this issue, as ads are generally sold by large, visible corporations. Finally, a data transaction tax may push smaller start-ups out of the business, because though larger companies may be able to internalize that cost, smaller companies that rely on advertising revenue to operate may lose customers because they cannot afford to take on the cost.[283] An ad valorem excise tax on *advertisements* would be more workable and likely more equitable.

C. Other Weaknesses

First, many have wondered: should we not simply ban the private collection of PII altogether? While this is probably impossible, the government could at least mandate certain deletion or deidentification requirements.[284] This would be an interesting solution, but at least until such is feasible, taxation will act as a stop-gap measure. Second, jurisdictional issues will arise insofar as businesses might incorporate overseas to avoid such a tax. While a valid objection, this argument is levied against most tax increases and has less to do with this particular proposal than persistent loopholes[285] in tax law writ large, which are beyond the purview of this

279. *See* Thimmesch, *supra* note 1, at 174–75. For example, Professor Thimmesch explains that, when one uses Google Docs, though "[a] user creates an account with an initial outlay of data, . . . [she] need pay nothing more if she does not use the product. Each time she does use the product, though, she receives a greater benefit and compensates Google with more data." *Id.* at 175.

280. *See* Bamberger, *supra* note 65, at 337; *See also* Thimmesch, *supra* note 1, at 179–80.

281. *See supra* Section IV.B.

282. *See* Thimmesch, *supra* note 1, at 180–82 (discussing how the anonymity of the internet makes it difficult to track down and tax data transactions).

283. *See, e.g.*, Walczak, *supra* note 12 (discussing small business concerns).

284. The GDPR does this for certain classes of data. *See generally At A Glance: De-Identification, Anonymization, and Pseudonymization under the GDPR*, BRYAN CAVE LEIGHTON PAISNER (July 24, 2017), https://www.bclplaw.com/en-US/insights/at-a-glance-de-identification-anonymization-and-pseudonymization-1.html [https://perma.cc/S6YK-493A].

285. *Fact Sheet*: *Offshore Corporate Loopholes*, AMS. FOR TAX FAIRNESS (2014), https://americansfortaxfairness.org/files/9-ATF-Offshore-Corporate-Tax-Loopholes-fact-sheet.pdf [https://perma.cc/J9M8-5AFZ].

Note. Finally, many have argued that the cost of a digital advertising tax will fall disproportionately on small businesses.[286] Though this is worrisome, a CCPA-like restriction on how, and to whom, the tax applies could be utilized.[287] However, this could further complicate the *Sorrell* issue and should be avoided unless the burden on small businesses is egregious.

CONCLUSION

We have entered the Information Age and are constantly restructuring old legal rules to create a more equitable and just society. Tax law, in particular, is an old tool that can help us address new, invasive harms. Tax law accepts that while it cannot change consumer preference, it can (1) disincentivize platforms from engaging in pernicious, invasive data collection; (2) help pay for the damage wrought by inevitable, massive data breaches; and (3) correct for the platform/user economic imbalance rife within our current system. While an excise tax on the sale of targeted digital ads created by the use of PII will not solve all of the data harms of the twenty-first century, it will at least move us closer to a functional framework of digital rights and harms.

Alida F. Babcock[*]

286. *See* Walczak, *supra* note 12.

287. *See California Consumer Privacy Act (CCPA)*, *supra* note 74. The CCPA only applies to for-profit businesses that do business in California and meet any of the following: have a gross annual revenue of over $25 million; buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices; or derive 50% or more of their annual revenue from selling California residents' personal information. *Id.*

* J.D. (2022), Washington University School of Law. Thank you to everyone on the *Washington University Law Review* staff, and a special thanks to Samuel Zachry, who graciously put up with my 12 AM calls about tax policy.