UNIVERSITY OF PITTSBURGH LAW REVIEW
Vol. 83 ● Summer 2022

NOTES

OTHER PEOPLE'S DATA: PRIVACY, ANTITRUST, AND THE BEHAVIORAL ADVERTISING BUSINESS MODEL

Isaac Joseph

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

NOTES

OTHER PEOPLE'S DATA: PRIVACY, ANTITRUST, AND THE BEHAVIORAL ADVERTISING BUSINESS MODEL

Isaac Joseph*

The goose that lays golden eggs has been considered a most valuable possession. But even more profitable is the privilege of taking the golden eggs laid by somebody else's goose.[1]

INTRODUCTION

Increasingly, consumers spend more and more of their time online. It is almost impossible to imagine how consumers can meaningfully participate in modern society without the internet. However, despite the amazing benefits and convenience that the internet and internet platforms provide in our daily lives, there looms in the background the ever more pressing question of consumer privacy—a question that the United States legal system has failed to address seriously as of yet. This is not to say that lawmakers and legal scholars have been ignorant of the question of consumer privacy. On the contrary, ever since the development of early computers and data processing in the 1950s, principles of consumer privacy and privacy legislation have been thrown around.[2] Even earlier than that, in 1890, Justices Warren and Brandeis

* J.D., 2022, University of Pittsburgh School of Law; B.A., 2018, University of Pittsburgh. I would like to thank my family and friends for all their support and encouragement throughout my years at the University of Pittsburgh.

[1] LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 17–18 (1914).

[2] John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)*, 66 CLEV. ST. L. REV. 559, 564–65 (2018).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

penned their seminal article on the right to privacy.[3] But despite more than a century of scholarship, American consumers are still locked in a struggle to protect their privacy from large data corporations like Amazon, Google, and Facebook. This is because an essential ingredient is missing from the privacy equation.

A committee, tasked by Congress in 2019 to investigate these data trusts, found that "these firms wield their dominance in ways that erode entrepreneurship, degrade Americans' privacy online, and undermine the vibrancy of the free and diverse press."[4] Indeed, one study, which tracked the changes in Facebook's stated privacy policy, found that its privacy protection measures slowly deteriorated between 2005 and 2015.[5] The most precipitous decline in Facebook's privacy protections and the corresponding increase in consumer surveillance came after 2014—uncoincidentally—once all of Facebook's social media competitors had exited the market.[6] The implication here is that the market power of dominant online platforms is interrelated to the problem of consumer privacy online. Thus, this Note argues that the current privacy framework has failed to protect consumer privacy because data privacy depends, in large part, on a corresponding antimonopoly framework that adequately addresses the competitive organization of an online economy fueled by data collection.

The Federal Trade Commission ("FTC") has rejected using antitrust law to approach data privacy issues because it maintains that consumer privacy protection and antitrust have separate objectives.[7] This rejection can be explained to the extent that it relies on an antitrust framework that is ill-equipped to deal with the new competitive harms brought by the emergent data industry. The naivete of continuing to conceptualize consumer privacy protection and antitrust as separate and mutually exclusive fields of law puts both consumer privacy and our economic structure in

[3] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[4] MAJORITY STAFF OF H.R. SUBCOMM. ON ANTITRUST, 116TH CONG., INVESTIGATION OF COMPETITION IN DIGITAL MARKETS 7 (2020) [hereinafter CONGRESSIONAL REPORT].

[5] Jennifer Shore & Jill Steinman, *Did You Really Agree to That? The Evolution of Facebook's Privacy Policy*, TECH. SCI. (Aug. 10, 2015), https://techscience.org/a/2015081102/ [https://perma.cc/S4BE-9HZD].

[6] Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 BERKELEY BUS. L.J. 39, 69–73 (2019).

[7] *See generally* Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 ANTITRUST L.J. 121 (2015) (arguing that the FTC has historically separated consumer protection and antitrust law because they have different objectives).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

jeopardy.[8] For decades, antitrust has been dominated by the theories of Law and Economics scholars, which focus on efficiency and neoclassical economic policies.[9] However, the failures of this antitrust regime to address the competitive organization of the internet economy have led many to criticize it and call for the antitrust regime to play a greater role in consumer privacy.[10]

Coincidentally (or perhaps by no coincidence at all), Law and Economics rejects privacy as an impediment to both innovation and efficiency in a free market system.[11] Contrary to this view, Professor Ryan Calo argues that privacy and the free market are actually quite complementary and support each other in a variety of ways.[12] In fact, privacy is an implicit assumption necessary for the proper functioning of the free market.[13] Privacy helps the free market efficiently allocate goods and services because, without privacy, goods and services would be allocated according to extraneous and salient information that is irrelevant to price and quality.[14] Privacy also allows market participants to build trust with each other in order to develop long-term economic relationships.[15]

If what Professor Calo posits is true, then it speaks to more than just a theoretical relationship between privacy and markets; it speaks to the coalescence of consumer privacy protection and antitrust law. It also raises some serious questions that privacy advocates have glossed over in their charge to demand more privacy protection laws. If privacy and trust are necessary components of a free market exchange, then why do companies like Facebook and Amazon not feel compelled to offer them? And if so many people are upset with the way such companies handle their privacy, why do they keep using their services? Put more simply, why is the market for privacy and data not self-regulating?

---

[8] *See* Pamela Jones Harbour & Tara Isa Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 76 ANTITRUST L.J. 769, 773–74 (2010); *see also* Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1009–11 (2013).

[9] *See* Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 740 (2017) (criticizing the current antitrust regime's ability to deal with digital platforms like Amazon and advocating for reform).

[10] *See id.*; *see also* Harbour & Koslov, *supra* note 8; *see generally* MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY (2016).

[11] Ryan Calo, *Privacy and Markets: A Love Story*, 91 NOTRE DAME L. REV. 649, 655–56 (2015).

[12] *Id.* at 650.

[13] *Id.* at 667–68.

[14] *Id.*

[15] *Id.* at 669–70.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

In Part I, this Note argues that the current privacy regulatory framework fails to meaningfully protect consumer privacy because consumers are unable to exercise autonomy in the privacy trade. Part II discusses the missing link to discussions about privacy, antitrust law, and how behavioral advertising prevents consumers from exercising privacy autonomy due to its subversion of the current antitrust framework. Part III argues that the potential harms from behavioral advertisement extend beyond merely invading consumers' privacy to manipulating their consumptive behavior. This has the potential to result in market failure, and our understanding of antitrust must change to account for this. Ultimately, this Note concludes by proposing that banning or severely restricting the online behavioral advertising business model is necessary to achieve both privacy and a free market.

I. FAILURE OF THE CURRENT FRAMEWORK

A. The Notice and Choice Framework

Currently, there are no comprehensive privacy laws in the United States. Instead, consumer privacy is regulated by a patchwork of laws, regulations, and government enforcement actions.[16] This system has been described as sectoral, in that a given privacy law will address only the specific privacy concerns of a sector or industry.[17] The most important of these, for the purposes of this Note, is the way in which the FTC has regulated consumer privacy online through Section 5 of the FTC Act, and particularly in the context of online platforms and behavioral advertising. Central to this framework are the guiding principles of notice and choice.[18]

Notice and choice is not a statutory or rigid regulatory model but manifests through guidance issued by the FTC, which advises websites and online platforms on how best to self-regulate consumer privacy.[19] The purpose of the FTC's now very-outdated online behavioral advertising principles is "to guide industry in developing more meaningful and effective self-regulatory models than had been developed to date."[20] Thus, the bedrock of the FTC's regulatory principles is the ability of internet

[16] Rothchild, *supra* note 2, at 582–83.

[17] *Id.*

[18] *See id.* at 561–62.

[19] *See, e.g.*, FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009) [hereinafter FTC REGULATORY PRINCIPLES].

[20] *Id.* at 11.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

platforms to self-govern while, at the same time, expecting consumers to make smart and informed choices. As such, "[t]he notice and choice mechanism is designed to put individuals in charge of the collection and use of their personal information."[21]

Looking more closely at the FTC's regulatory principles, however, reveals that the scope of the decision-making contemplated by the FTC is actually quite narrow; and the nexus of the consumer's choice comes down to the website or platform's privacy policy, which is a statement that ostensibly informs the consumer about the website's information collection practices.[22] This is reflected in the circumscribed types of claims that are brought to enforce the notice and choice framework. Notice and choice can be enforced by the FTC under Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices."[23] In 2014, a team of law professors collected and categorized all the federal class action complaints filed against the FTC by private parties and the FTC's enforcement actions under the notice and choice framework from the ten years prior. The authors organized the complaint data and categorized "[t]he harms that were most frequently asserted . . . : (1) unauthorized disclosure of personal information, (2) surreptitious collection of personal information, (3) failure to secure personal information, and (4) unlawful retention of personal information."[24] Whereas type three focuses on cybersecurity claims, types one, two, and four can effectively be lumped into one category: claims dictated by the contours of the privacy policy. Although these claims sound like those that are found in contract law because there is a promise (notice), acceptance (choice), and a failure to adhere to the promise (breach)—notice and choice is decidedly noncontractual, and privacy policies are nonbinding.[25]

In contrast to this narrow scope of privacy harms that are actionable under the notice and choice framework, Professors Danielle Citron and Daniel Solove

---

[21] Joel R. Reidenberg, N. Cameron Russel, Alexander Callen, Sophia Quasir & Thomas Norton, *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: J.L. & POL'Y 485, 489 (2015).

[22] *See, e.g.*, FTC REGULATORY PRINCIPLES, *supra* note 19, at 30 (recommending, but not requiring, that websites which collect consumer data for behavioral advertising should not only give notice about such collection and use but to allow consumers to "*choose whether to allow such collection and use*") (emphasis added). The ability to give consumers that choice lies entirely with the website. Imagine running a brick-and-mortar store and the FTC recommends that you allow consumers the option not to pay you for your goods. Would you give them that option?

[23] 15 U.S.C. § 45(a)(1).

[24] Reidenberg, Russel, Callen, Quasir & Norton, *supra* note 21, at 512.

[25] Thomas B. Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 181, 185 (2016).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

characterize a wide range of potential privacy harms not captured by the current framework.[26] Among these are harms to autonomy—like coercion and manipulation, and discrimination harms.[27] As discussed further below, autonomy and discrimination harms are endemic to the behavioral advertising and data collection business model. The Health Insurance Portability and Accountability Act ("HIPAA") is an example of a privacy law that prohibits medical providers from conditioning treatment on collecting and selling patient data for advertising purposes.[28] Because of the necessity of healthcare to daily life, HIPAA recognizes that data collection practices can be coercive or manipulative of consumers' behavior and choice to access healthcare.[29] Notice and choice, on the other hand, fails to take that step.

Importantly, the contours of any given privacy policy, and indeed whether one exists at all, are determined by the extent to which the notice and choice framework—or, in its absence, the free market—regulates contractual/transactional relationships between consumers and websites. Although notice and choice is a largely self-regulatory approach[30] (i.e., relies on the free market), it also attempts to regulate this transactional relationship through its operation as a default rule.[31] The law of incomplete contracts is premised on the theory that contracting parties, especially in daily, routine transactions, do not have the time or resources to negotiate every provision or aspect of the bargain.[32] In this absence, default rules operate to provide the terms, by operation of law, to which the contracting parties would have agreed had they the time or resources to negotiate them.[33] Janger and Schwartz would likely categorize notice and choice as a kind of information forcing default, in the same way that the Gramm-Leach-Bliley Act implements those principles.[34] Information forcing defaults attempt to cure situations in which there is an

[26] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 797 (2022).

[27] *Id.* at 846, 855.

[28] *Id.* at 846.

[29] *Id.*

[30] *See* FTC REGULATORY PRINCIPLES, *supra* note 19, at 11.

[31] *See* Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1232–33 (2002).

[32] *Id.* at 1233–34.

[33] *Id.* at 1233–35.

[34] *See id.* at 1239.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

information asymmetry between the contracting parties by "forcing" one party to fully inform the other of material information affecting the transaction.[35] Notice and choice does precisely this; it forces websites and platforms to divulge their information collection practices so that consumers can be fully informed about the privacy implications before engaging.

A prime example of information forcing defaults are "lemon" laws. The "lemons" dilemma is one where a consumer is looking to purchase a product, often a used car, about which they know nothing save for the price.[36] Although there is nonprice information about the car that is pertinent to the consumer, it is either impossible or too costly to acquire, and so the consumer does not know whether the car they are purchasing is in good shape or if it is a "lemon," and is substantially defective.[37] In this situation, the consumer chooses which car to buy based on price, not quality, since this is the only information they have access to.[38] This means the consumer will invariably choose the lower-priced car with faulty mechanics rather than the higher-priced car with good mechanics in every case, which drives all the good quality cars out of business.[39] Thus, information forcing defaults, like the lemon laws, require car dealers to give the consumers notice of the car's mechanical specifications in order to balance the information asymmetry and allow the consumer to purchase a quality car for a reasonable price.[40]

Turning this analytical framework to the online marketplace, we should see that notice and choice allows consumers to see important nonprice aspects of the trade, such as whether a website collects user information to sell for advertising and to be able to choose higher-priced services that offer more favorable terms, such as not collecting your information. Yet, it becomes clear that consumer privacy is still in a lemons dilemma. Despite the fact that websites and platforms lay their privacy policies bare, virtually no consumer reads these policies before "choosing" to accept them.[41] Thus, even though consumers have the necessary nonprice information, they

[35] *Id.*

[36] *Id.* at 1240.

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *See* Daniel Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 1 (2021); Rothchild, *supra* note 2, at 628.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

still choose the free services of Facebook and Google, rather than pay for a service that offers better privacy terms (i.e., one that does not use behavioral advertising to finance its business). But this does not necessarily mean that consumers uniformly disvalue their privacy. For example, one study of Gmail users found that most users thought the service was highly intrusive, yet only thirty-five percent said they were willing to pay for a more private email service.[42] What are we to make of this?

B. Why Notice and Choice Fails

The phenomenon whereby consumers claim to value their personal data privacy but readily give it up in exchange for free online services presents a veritable paradox. There are at least two diverging views about why this happens. Some take the behavioral valuation approach, arguing that people's actual behaviors are an accurate measure of how much they value their own privacy.[43] Consumers simply do not value their privacy, or else they would pay for it. In this view, there is no failure in either the notice and choice or antitrust frameworks because the privacy trade is being properly mediated by the free market.[44] Importantly, this view assumes that consumers are fully informed and have a wide array of competitive options.[45] However, considerably lacking in the online marketplace is any array of options, which means that consumers are not able to exercise choice regardless of how informed they are that the websites they visit will be spying on them.[46] For example, the top twenty-five most visited commercial websites have almost uniform privacy policies which allow the websites to collect personal data and sell it for behavioral advertising.[47] This is a tell-tale sign of a market for lemons.

This suggests not just a failure of notice and choice, but of antitrust as well. Because of this dearth in options, "[c]onsumers neither experience nor hope for meaningful protection of privacy in the 'terms of service' foisted on them . . . ."[48] This is not to say that consumers cannot expect that privacy policies will protect them in other ways, such as by penalizing a company for collecting or selling personal

[42] Solove, *supra* note 41, at 9.

[43] *Id.* at 11.

[44] *Id.* at 12.

[45] STUCKE & GRUNES, *supra* note 10, at 58.

[46] Rothchild, *supra* note 2, at 621.

[47] *Id.* at 621–24.

[48] Pasquale, *supra* note 8, at 1012.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

data in a way that it was not formalistically authorized to do under the policy, but they fail to protect a consumer's choice to access the internet without having to engage in the privacy trade at all.[49] "[A] consumer's options are either to accept the industry-standard privacy-invasive practices or stay off the Internet."[50] The FTC has also regulated privacy policies to the extent that it has charged companies with unfair practices if their privacy policies diverge too far from the industry standard.[51] However, since these enforcement practices do not consider the effects of market monopolization, industry standards cease to be a useful benchmark if they continue to deteriorate in the absence of competition.[52]

Because this FTC regime refuses to treat privacy and antitrust as coincident issues,[53] it therefore fails to differentiate whether consumers' continued use of online platforms, like Facebook, reflects an overwhelming consumer preference for these privacy-invasive platforms or a desperate lack of choice.[54] Indeed, many proponents of the current regime fail to see the lemons dilemma at all because they consider privacy invasion to be an improvement in quality, rather than a deterioration, due to its ability to bring better content and services tailored to consumers as well as efficient behavioral advertising.[55] Adding further to this complex wrinkle is the issue that there may be several stronger and non-substitutable factors motivating a consumer's decision to use a particular internet service, such as the content of the site or how tailored the service is (which is, again, achievable largely through privacy invasion),[56] rather than choosing another service based merely on the existence of a better privacy policy.[57]

---

[49] Rothchild, *supra* note 2, at 627.

[50] *Id.*

[51] Pasquale, *supra* note 8, at 1016; *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FTC (May 2021). https://www.ftc.gov/about-ftc/mission/enforcement-authority [https://perma.cc/W78R-M84R].

[52] *Id.* at 1016–17.

[53] Ohlhausen & Okuliar, *supra* note 7, at 138.

[54] Pasquale, *supra* note 8, at 1014.

[55] James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129, 1130 (2013); Ohlhausen & Okuliar, *supra* note 7, at 131.

[56] Pasquale, *supra* note 8, at 1014–15.

[57] *Id.* at 1015; Rothchild, *supra* note 2, at 627–28.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

The behavioral valuation approach is also problematic because it is a relatively simplistic view of human behavior that assumes perfect rationality. The other view of the privacy paradox accepts that consumers can sometimes behave irrationally based on biases, such as the need for the instant gratification Google search queries provide by giving you immediate knowledge right at the moment you desire it rather than wholeheartedly balancing the value of one's own privacy.[58] The privacy trade is also distorted because consumers may not fully understand the extent to which their privacy is collected and sold to advertisers, or the fact that online platforms are intentionally designed to manipulate behavior and distort perceptions of risk.[59] Moreover, consumers often are unable to overcome the inertia of default settings that allow information collection automatically or the need to repeatedly change default settings in order to prevent data collection.[60] Ironically, as an information forcing default, notice and choice may itself result in information overload, whereby a consumer is overwhelmed by the information in the privacy policy and thus relies instead on heuristics, biases, and rules of thumb to make a decision.[61]

Daniel Solove goes further to argue that the privacy paradox does not exist; people's behavior with respect to their privacy online has nothing to do with valuations or actual preferences but reflects risk assessment in a very specific set of circumstances.[62] When consumers make the choice to share information online, they are weighing the possible downstream consequences of doing so.[63] Consumers decide based on their assumptions about what a third party might use their information for and the likelihood of that happening.[64] As such, although people's behavior demonstrates that they are unwilling or unable to protect their data privacy online, Solove concludes that this does not mean that consumers do not value privacy generally or that privacy regulation is not needed.[65] "[P]rivacy is not a product[, it]

[58] *Id.* at 15–16.

[59] *Id.* at 18–20.

[60] STUCKE & GRUNES, *supra* note 10, at 58–59.

[61] Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1012 (2014).

[62] Solove, *supra* note 41, at 23.

[63] *Id.* at 25.

[64] *Id.* at 26–27.

[65] *Id.* at 26, 31.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

has a value beyond what people will pay for it."[66] Beyond its ability to purchase free internet services, privacy serves as a foundation for a free and democratic society because it helps to limit governmental and economic power, maintain appropriate social boundaries, foster trust, and protect freedom of speech.[67]

Perhaps more concerning, the blame for many of these irrational behaviors cannot be laid solely at the feet of consumers' own psychological shortcomings but also at the feet of dominant platforms that design their platforms and tailor their content to deliberately trigger addiction and dependency from consumers without their realizing it.[68] These tactics are called dark patterns and they are designed to subvert a consumer's ability to exercise autonomy in the online marketplace.[69] To understand why platforms resort to these tactics, one must understand the essential building block of the behavioral advertising business model: monetizing user attention.[70] Advertising is a simple and effective way to turn attention into money since the time consumers spend looking at advertisements while perusing Instagram is valuable to advertisers.[71] Even in Facebook's submissions to the Antitrust Subcommittee for its report, it explained that it faces "intense competition" for users' attention from other websites and apps, such as YouTube and mobile games.[72] However, attention is not only valuable because it puts eyeballs on advertisements but also because every minute a consumer spends on a platform is an additional minute for personal data to be collected and analyzed for targeted ads.[73] And the best part is that the very same data can be used to create tailored and suggested content to keep users engaged for longer.[74]

---

[66] *Id.* at 35; *see also id.* at 37 ("Attempts to place a monetary value on personal data are doomed to be completely inaccurate as a metric of anything meaningful. The monetary amount placed on privacy does not reflect privacy's value; at best it reflects a risk assessment, which is infected by behavioral distortions and not able to be performed in a meaningful way due to lack of knowledge or lack of choice.").

[67] *Id.* at 38–40.

[68] Gregory Day & Abbey Stemler, *Are Dark Patterns Anticompetitive?*, 72 ALA. L. REV. 1, 4 (2020).

[69] *Id.*

[70] *Id.* at 8.

[71] *Id.*

[72] CONGRESSIONAL REPORT, *supra* note 4, at 135.

[73] Day & Stemler, *supra* note 68, at 8–9.

[74] *Id.* at 9.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

The ultimate problem, though, is finding where to draw the line between creating a great product that consumers enjoy and choose to spend their time on and subverting consumer autonomy by manipulating their behavior. For example, some of the design features of these dominant platforms that we take for granted, such as infinite scrolling on your feed or the timing of notifications, purposefully create random intervals of positive stimuli which release dopamine in the brain.[75] The random release of dopamine is akin to the effects of gambling addiction, creating a cycle of dependency on the platform.[76]

The most recent Facebook scandal involving the Capitol riot on January 6, 2021, has highlighted yet another problematic scheme to increase user attention: the reckless, if not intentional, algorithmic promotion of radicalizing content, misinformation, and conspiracies to keep users engaged.[77] Scholarship on the subject has noted that one possible side effect of tailoring content to users' perceived preferences is that it may lead—and indeed already has led—to increased political polarization.[78] For example, in constructing categories of consumer profiles for businesses to target them with behavioral ads, Facebook offered the following profiles: "'opposition to immigration'; 'far left politics'; 'vaccine controversies'; and 'climate change denial.'"[79]

Aside from promoting addiction and toxicity to keep users' attention on the platform, dark patterns can also subvert user autonomy by subtly influencing them to surrender their privacy.[80] For example, a platform may use manipulative designs

[75] *Id.* at 12–13.

[76] *Id.* at 13–14.

[77] AM. ECON. LIBERTIES PROJECT, HOW TO PREVENT THE NEXT SOCIAL MEDIA-DRIVEN ATTACK ON DEMOCRACY—AND AVOID A BIG TECH CENSORSHIP REGIME 3 (2021), https://www.economicliberties.us/wp-content/uploads/2021/02/Corporate-Power-Quick-Takes_4.pdf [https://perma.cc/CH9U-9YAL].

[78] Calo, *supra* note 61, at 1006; *see also* Paul Barrett, Justin Hendrix & Grant Sims, *How Tech Platforms Fuel U.S. Political Polarization and What Government Can Do About It*, BROOKINGS (Sept. 27, 2021), https://www.brookings.edu/blog/techtank/2021/09/27/how-tech-platforms-fuel-u-s-political-polarization-and-what-government-can-do-about-it/ [https://perma.cc/MH9N-5SP5]; Isaac Stanley-Becker, *Facebook's Ad Tools Subsidize Partisanship, Research Shows. And Campaigns May Not Even Know It*, WASH. POST (Dec. 10, 2019, 8:00 AM), https://www.washingtonpost.com/technology/2019/12/10/facebooks-ad-delivery-system-drives-partisanship-even-if-campaigns-dont-want-it-new-research-shows/ [https://perma.cc/PRX5-PCCA].

[79] Jeannie Marie Paterson et al., *The Hidden Harms of Targeted Advertising by Algorithm and Interventions from the Consumer Protection Toolkit*, 9 INT'L J. CONSUMER L. & PRAC. 1, 8 (2021).

[80] Day & Stemler, *supra* note 68, at 14–15.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

that prey on cognitive biases to steer consumers away from changing privacy settings.[81] Although it did not explicitly recognize it as such at the time, the FTC has already brought a deceptive practice action against Facebook for use of dark patterns to deceive consumers into thinking that their private information was not being shared with Cambridge Analytica.[82] However, deception is but one tool in the dark pattern arsenal, and bringing an enforcement action for deceptive practices under the FTC Act will not be enough to halt different kinds of manipulative practices.[83]

Thus, returning to the idea of the privacy paradox, we can see that consumers lack a considerable amount of autonomy in the online privacy trade despite their knowledge of information collection practices through notice and choice. Consumers evidently are unable or unwilling to protect their privacy in the face of this information. This is due to a wide array of factors, from consumers' cognitive biases to intentionally manipulative designs, that subverts consumers' freedom of choice. In turn, the online marketplace remains in a lemons dilemma which prevents competitive alternatives to the privacy trade from emerging and succeeding. Thus, data collection, and the behavioral advertising business model underwriting the internet writ large, concerns not merely consumer protection, but the very state of competition on the internet. Enter our missing ingredient to the privacy trade: antitrust. Without an understanding of how behavioral advertising subverts current antitrust law, we will never get to the point of understanding what tools we really need to effectively protect consumer privacy online.

II. THE ROLE OF ANTITRUST

Since the enactment of the Sherman Antitrust Act, antitrust law has evolved to be predominantly guided by neoclassical economic (read: Law and Economics) policy, dubbed the Chicago School, which emphasizes the efficiency of markets above all else.[84] This approach to antitrust resonates more with Law and Economics' hostility towards privacy as an impediment to efficiency than with the codependence

[81] *Id.* Likewise, as discussed earlier, consumers' irrationality and biases may lead them to favor the instant gratification of finding the answer to their question on Google rather than overcome the inertia of turning off default data collection settings first.

[82] Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/HK3A-E92R].

[83] Day & Stemler, *supra* note 68, at 22–23.

[84] Khan, *supra* note 9, at 717–19; Ohlhausen & Okuliar, *supra* note 7, at 143.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

of privacy and free markets that Calo advocates.[85] Indeed, one argument against addressing privacy concerns through antitrust law is that it would hamper the free flow of information between sellers and buyers which restricts efficient outcomes and may even impinge on commercial free speech protected by the First Amendment.[86] The current antitrust regime, as such, sees no problem with companies like Amazon, Facebook, and Google dominating the market precisely because it reflects and also results in greater efficiency.[87] When viewed from the lens of efficiency, extensive data collection is seen as beneficial to consumer welfare because it improves the ability of the platform to provide content and services to consumers while delivering strikingly efficient targeted advertising.[88] Offering their platforms for free makes these companies all the more elusive to this antitrust framework.[89]

Most importantly, in the context of online behavioral advertising and markets for data, the Chicago School has (a) narrowed the concept of entry barriers, which are the costs that new market entrants must bear to compete against already-established firms;[90] and (b) greatly diminished scrutiny of anticompetitive mergers.[91]

A. Entry Barriers

The dismissal of entry barriers as an anti-competitive concern by the Chicago School is a key element of the view that "market power is always fleeting,"[92] and that a large market share today does not represent a monopoly power that will be here tomorrow. This idea rests on the Schumpeterian theory in economics that

[85] *See* Calo, *supra* note 11, at 655.

[86] Cooper, *supra* note 55, at 1140.

[87] Khan, *supra* note 9, at 744 ("The modern view of integration largely assumes away barriers to entry, an element of structure, presuming that any advantages enjoyed by the integrated firm trace back to efficiencies.").

[88] Ohlhausen & Okuliar, *supra* note 7, at 131; Cooper, *supra* note 55, at 1130.

[89] Nathan Newman, *Search, Antitrust, and the Economics of the Control of User Data*, 31 YALE J. ON REGUL. 401, 412 (2014); Srinivasan, *supra* note 6, at 44.

[90] Khan, *supra* note 9, at 719–20.

[91] *See* Herbert J. Hovenkamp, *Schumpeterian Competition and Antitrust*, PENN L.: LEGAL SCHOLARSHIP REPOSITORY (Oct. 15, 2008), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2790&context=faculty_scholarship [https://perma.cc/8S5H-DAPR].

[92] Khan, *supra* note 9, at 719–20.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

technological innovators compete *for* the market, but not *within* the market.[93] That is, technological innovators like Facebook and Google will come to dominate the market initially but must compete against successive innovators who will come to dominate the market after them.[94] In a market characterized by low entry barriers, competitors are—theoretically—easily able to contest a monopolist if it attempts to use market power.[95] Thus, the Chicago School has circumscribed the set of circumstances sufficient to show an exercise of market power, so long as that market has low entry barriers.

Since it is relatively easy to design and launch an app, with standardized and widely available technology, entry barriers to the market are seemingly low.[96] Thus, any innovator with a popular idea should easily be able to sweep the market from those who currently dominate it.[97] However, the reality is that the dominant platforms' wealthy stores of consumer data—which is what makes user attention valuable and what motivates the erosion of privacy—act as a steep entry barrier to any would-be innovator or market entrant.[98]

Professor John Yun argues, from the Chicago School perspective, that data itself is not even necessary for innovators to overtake the market—all they need is a clever idea and a chip on their shoulder.[99] As such, Professor Yun does not believe that the input cost of acquiring large troves of data is enough to label it an entry barrier.[100] However, a quick survey of how data functions in the behavioral advertising industry will demonstrate otherwise.

To overcome entry barriers within the search advertising market, which Google dominates, a potential competitor must generate enough revenue from advertising to outweigh the fixed costs of running an internet browsing service, such as physical

[93] Michael Katz, *Multisided Platforms, Big Data, and a Little Antitrust Policy*, 54 REV. INDUS. ORG. 695, 705 (2019); Spencer Waller, *Antitrust and Social Networking*, 90 N.C. L. REV. 1771, 1800–01 (2012).

[94] Waller, *supra* note 93, at 1801–02.

[95] Amanda Reeves & Maurice Stucke, *Behavioral Antitrust*, 86 IND. L.J. 1527, 1554–55 (2011).

[96] STUCKE & GRUNES, *supra* note 10, at 159.

[97] *Id.*

[98] Newman, *supra* note 89, at 420.

[99] John M. Yun, *Antitrust After Big Data*, 4 CRITERION J. ON INNOVATION 407, 415–17 (2019).

[100] *Id.* at 421–22.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

sites that house servers to store data and an army of programmers.[101] It should come as no surprise that Google's ability to charge exorbitant rates on advertisers, thus generating enough revenue to outweigh its fixed costs, is due to the scope and scale of its consumer data; the more data Google can sell advertisers, the more likely advertisers can target the right consumers to buy their product.[102] Therefore, Google's control of data to the exclusion of others is an entry barrier, not because fixed costs prevent entry necessarily, but because it prevents charging the premium on behavioral advertising that would make competition viable.[103] This means being able to spend the same or more on fixed costs—to develop a state-of-the-art algorithm, even—will be of no use to a competitor if it cannot generate revenue like Google.[104]

The extent to which data acts as an entry barrier can be illustrated by the example of Bing. In considering the importance of data to competition in search advertising, the DOJ cleared Microsoft's acquisition of Yahoo! to combine their data and ostensibly to create greater competition with Google through Microsoft's search browser, Bing.[105] Despite this, Microsoft still loses billions of dollars annually towards building and operating Bing because it can only charge advertisers a fraction of what Google can.[106] Because of Google's exclusive control over consumer data, many advertisers are compelled to advertise with Google.[107] This is also true of Facebook—the House Antitrust Subcommittee found that many marketers feel compelled to advertise through Facebook because of the scale of its data and reach to users.[108] If Microsoft, a tech giant with its own fair share of antitrust violations, cannot keep its search engine financially viable in the face of Google, who can?

Despite this market dynamic, Law and Economics pundits, like Professor Yun, persist in their conviction that entry barriers do not exist in the digital market. He posits:

---

[101] Newman, *supra* note 89, at 418–19.

[102] *Id.* at 420.

[103] *Id.* at 421.

[104] *Id.*

[105] Ohlhausen & Okuliar, *supra* note 7, at 143–44.

[106] STUCKE & GRUNES, *supra* note 10, at 7; Newman, *supra* note 89, at 418.

[107] Newman, *supra* note 89, at 421–22.

[108] CONGRESSIONAL REPORT, *supra* note 4, at 170–71.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

> [W]e should not be narrowly focused on a particular product or approach a firm uses—for example, one that involves use of a certain volume or type of big data in particular ways—but on the larger question of whether other viable approaches to entry are hindered and, as stated earlier, whether this hindrance results in a loss of welfare.[109]

Essentially, Professor Yun's argument is that barriers to entry do not exist merely when nobody can challenge Google using the behavioral advertising business model, but when nobody can challenge Google using a more innovative product or model.[110] Quite so.

In fact, Google's business model, which relies on offering free services and monetizing users' data, creates an entry barrier in such a way that competing by using any other business model, innovation aside, is impractical.[111] The House Antitrust Subcommittee found that many start-ups feel compelled to use behavioral advertising as a business model because there is no other way to gain revenue and attract users online.[112] Because companies like Google and Facebook have set the competitive market price for their services at zero, this prevents any entrant from using a business model that may charge consumers directly.[113] Any entrant wishing to offer better privacy is easily outcompeted because this necessarily entails not exploiting data for profit.[114] The current regime also fails to recognize the competitive harm of dominant platforms exploiting consumer data and using psychological biases to keep users addicted to these platforms and distort their perception of privacy risks.[115] Any entrant wishing to respect consumers' privacy and autonomy might find it impossible to win over any users in the face of the dominant firm's manipulative practices.[116] Yun misses the point because big data is not just a barrier to entry because it represents an input cost for firms wishing to

---

[109] Yun, *supra* note 99, at 422.

[110] *Id.* at 422–23.

[111] Newman, *supra* note 89, at 412.

[112] CONGRESSIONAL REPORT, *supra* note 4, at 171.

[113] Newman, *supra* note 89, at 412; STUCKE & GRUNES, *supra* note 10, at 160.

[114] ALEX MARTHEWS & CATHERINE TUCKER, PRIVACY POLICY AND COMPETITION 7 (2019), https://www.brookings.edu/wp-content/uploads/2019/12/ES-12.07.19-Marthews-Tucker.pdf [https://perma.cc/SWZ9-Z85J].

[115] *See* Calo, *supra* note 61, at 1001.

[116] *Id.* ("[I]f some market actors leverage bias, those that do not could be edged out of the market.").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

utilize it, but because it is wielded to such dominant ends by platform monopolies, that even firms not wishing to use data are hampered.

Professor Yun would argue further that, even if it is more difficult for firms with these kinds of business models to enter the market, there is still no competitive problem because there is no harm to consumer welfare since the Chicago School views consumer welfare strictly in terms of price.[117] The Chicago School's idea of consumer welfare, short-sighted as it is, would consider competitive options that charge consumers but do not collect their data to be worse for consumers than the free option that Google provides. Thus, the lemons dilemma persists because, as discussed in the previous section, cognitive biases and manipulation prevent consumers from choosing to pay for privacy, which in turn reinforces data collection and behavioral advertising as the only viable business model. The cycle then continues, as consumers simply cannot make informed privacy decisions when no options other than surveillance exist.

B. Anticompetitive Acquisitions

Because the data entry barrier is too steep to directly compete with incumbents, the only way a competitor can hope to compete is by entering an adjacent market in order to start acquiring enough consumer data to present a competitive threat to the incumbent when it moves into that incumbent's market.[118] The incumbents will often acquire these adjacent entrants before they become a competitive threat, and because they are not direct competitors *yet*, these acquisitions do not draw scrutiny from antitrust authorities.[119] Perhaps they should.

The problem, however, is that it is almost impossible for economists, let alone federal judges, to predict which entrants into the market will become the successful

[117] Yun, *supra* note 99, at 422 ("[W]hether other viable approaches to entry are hindered and . . . *whether this hindrance results in a loss of welfare*.") (emphasis added).

[118] Novell, Inc. v. Microsoft Corp., 505 F.3d 302, 308 (4th Cir. 2007) ("[O]nce dominance is achieved, threats come largely from outside the dominated market, because the degree of dominance of such a market tends to become so extreme."); Katz, *supra* note 93.

[119] Katz, *supra* note 93; Tim Wu & Stuart A. Thompson, *The Roots of Big Tech Run Disturbingly Deep*, N.Y. TIMES (June 7, 2019), https://www.nytimes.com/interactive/2019/06/07/opinion/google-facebook-mergers-acquisitions-antitrust.html (noting that the federal government has challenged none of Facebook's 92 acquisitions and only challenged 3 of Google's 270 acquisitions, nevertheless ultimately approving all of them).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

innovators that create the Schumpeterian upsets.[120] The Chicago School prefers to face this puzzling task with skepticism and to let market forces play out rather than interfere.[121] Nevertheless, one can be sure that it is the dominant firms that are likely to be the victims of such upsets and, knowing this, will attempt to use their market power to suppress innovative entrants who may cause the upsets.[122] This is relatively easy to do because the innovations that threaten incumbency usually come from small firms and start-ups.[123] It is also expected that these incumbents will neither contribute to nor invest in any innovations themselves, preferring to rely on the steady profit growth of their current innovation, since there is no pressure to devise new innovations in the absence of competition.[124] This also chills investment in start-up ventures and innovations, especially when acquisition by a dominant firm is imminent.[125]

It was these anticompetitive acquisitions of nascent competitors that, in no small part, drove Google and Facebook to market dominance.[126] An often-critiqued example of this kind of practice is Facebook's acquisition of Instagram and WhatsApp, two nascent competitors in social networking, but it is by no means the only example.[127] In fact, the level of data privacy offered by WhatsApp in exchange for its free service was a key element in consumers' preference for the app.[128] Nevertheless, none of Facebook's ninety-two acquisitions since 2007 have been scrutinized by the federal government.[129] Google's parent corporation, Alphabet, is responsible for about 270 acquisitions, including direct competitors such as DoubleClick, YouTube, and Waze.[130]

---

[120] Hovenkamp, *supra* note 91, at 6; C. Scott Hemphill & Tim Wu, *Nascent Competitors*, 168 U. PA. L. REV. 1879, 1888 (2020) (illustrating the issue with the example of cell phones, which originally competed with landline telephones but unpredictably moved into markets for cameras and computers).

[121] Hovenkamp, *supra* note 91, at 3.

[122] *Id.* at 6.

[123] Hemphill & Wu, *supra* note 120, at 1887.

[124] Hovenkamp, *supra* note 91, at 7.

[125] CONGRESSIONAL REPORT, *supra* note 4, at 49.

[126] Wu & Thompson, *supra* note 119; Khan, *supra* note 9, at 783 n.376; Katz, *supra* note 93, at 705.

[127] Hemphill & Wu, *supra* note 120, at 1885–86.

[128] STUCKE & GRUNES, *supra* note 10, at 132.

[129] Wu & Thompson, *supra* note 119.

[130] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

If it is nearly impossible to predict which of these acquired innovators might have turned the market against the incumbents, how, then, did these incumbents know which ones presented a potential threat? Based on hearings and other fact-finding inquiries, the House Antitrust Subcommittee concluded that Facebook, for one, was able to use its vast trove of consumer data and algorithms to identify which new apps or platforms would present a competitive threat by tracking consumer trends.[131] In other words, Facebook's ability to surveil consumers' online activities gives it unprecedented power to predict which incipient firms are likely to be the competitors that upset the market. Thus, to respond in an alternative way to Professor Yun's argument—that we should focus "on the larger question of whether other viable approaches to entry are hindered"[132]—it is not only impossible for market innovators to enter the market directly, but also adjacently. As it turns out, an innovative idea and a chip on your shoulder are not sufficient conditions for sustained entry.

Facebook's explicit strategy, from internal documents, was to pressure these firms into selling.[133] In the case of Instagram, for example, Facebook pressured the up-and-coming photo-sharing app by cloning its features to make its own rival photo-sharing service and presenting Instagram's CEO with an ultimatum between acquisition or assured destruction.[134] Snapchat presents an example of what happens when a platform chooses to resist Facebook's overtures to purchase it. Facebook was able to clone Snapchat's "stories" feature and, by 2018, had twice as many users on its version of "stories" than Snapchat.[135]

The Chicago School still would not see a problem with this kind of activity since entry barriers are supposedly low enough that firms would continue to enter the market faster than incumbents could buy them out.[136] Even if we accept that entry barriers are low, this argument only works in theory and not in reality. In theory, yes, new messaging apps could continue to be developed even after Facebook has acquired WhatsApp, and Facebook cannot feasibly keep acquiring them all. But how many messaging apps are consumers expected to download onto their phones before

[131] CONGRESSIONAL REPORT, *supra* note 4, at 160–62.

[132] Yun, *supra* note 99, at 422.

[133] CONGRESSIONAL REPORT, *supra* note 4, at 163.

[134] *Id.* at 163–64.

[135] *Id.* at 164–65.

[136] *Id.* at 771; Yun, *supra* note 99, at 419.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

we reach that point? Three? Five? Twenty? Due to network effects, most consumers are already connected to their networks via Facebook and/or WhatsApp and are unlikely to download and get their entire network to migrate to the next app to come out.[137]

What this phenomenon reflects is the strength of each social networking app over a consumer's different social groups.[138] For example, I may use WhatsApp to talk with old high school friends but Facebook Messenger ("Messenger") to talk with family. The bottom line is that a consumer's choice to use Messenger rather than WhatsApp often reflects which social group they are communicating with (and over which that platform exerts network dominance) and in no way reflects the consumer's choice of quality or privacy preferences for the app.[139] Thus, while WhatsApp may have been a competitive restraint *before* its merger with Facebook, *after* the merger Facebook faced no competitive pressures from potential entrants that could challenge its position with better privacy because Facebook knew users would continue to be attached to WhatsApp by their network.[140] Tellingly, WhatsApp users did not organize a migration to any new apps, despite initially choosing WhatsApp for its privacy.[141]

Professors C.S. Hemphill and Tim Wu propose that antitrust enforcement should change to address this barrier to competition by blocking more of these types of mergers.[142] The principal difficulty in doing so is, of course, identifying such mergers.[143] Overenforcement by preventing mergers which may be benign can have the undesired effect of chilling venture capital for risky start-up innovators because acquisition by a larger firm is usually an exit for investors and helps incubate the start-up to be successful.[144] However, Wu and Hemphill propose that, rather than prove beyond all doubt that an acquired firm would have become a competitive threat, enforcers should be allowed to demonstrate a likelihood of such a threat and only scrutinize acquisitions by the most dominant firms to which a nascent

[137] STUCKE & GRUNES, *supra* note 10, at 168–69.

[138] *Id.* at 168.

[139] *Id.* at 168–69.

[140] *Id.* at 169.

[141] *Id.*

[142] Hemphill & Wu, *supra* note 120, at 1890–91.

[143] *Id.* at 1888.

[144] *Id.* at 1893.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

competitor is likely to pose a threat.[145] Such an inquiry should not even be necessary in cases where internal documents and communications show that the dominant firm's explicit motive for acquisition is to prevent competition, as in Facebook's case.[146]

III. WHY ANTITRUST MATTERS FOR UNDERSTANDING PRIVACY

A. The Connection Between Privacy and Competition

The key point of conflict between the Chicago School understanding of antitrust and those who seek antitrust reform is in their conception of antitrust law's ultimate purpose. Whereas the Chicago School has focused almost exclusively on efficiency as the metric for a justifiably competitive market, others believe a different paradigm should guide our understanding of competition.[147] Importantly, this unwavering devotion to efficiency has come with hostility towards privacy as an impediment to the free flow of information and the efficient functioning of markets.[148]

On its face, equating efficiency with competition is not apparently problematic, but once we start to consider the way in which competition, efficiency, and privacy interact with each other we see the equivalence begin to erode. If we accept Calo's proposition that privacy is a necessary component to the free market as a starting principle, we can conclude that privacy and efficiency are not diametrically opposed because the free market promotes the most efficient allocation of resources.[149] For the Chicago School, a monopolized or oligopolized market is not inherently problematic or anticompetitive because it can still promote allocative efficiency and consumer welfare.[150] Even so, there is yet a chasmic difference between one or two companies controlling the accumulation of monetary wealth in a market, and one or two companies controlling all the information in a market.

---

[145] *Id.* at 1890–91.

[146] *Id.* at 1905–06.

[147] *See* Lina Khan, *The New Brandeis Movement: America's Antimonopoly Debate*, 9 J. EUR. COMPETITION L. & PRAC. 131, 132 (2018) [hereinafter *The New Brandeis Movement*].

[148] Calo, *supra* note 11, at 655–56.

[149] *See id.* at 665.

[150] *The New Brandeis Movement*, *supra* note 147, at 132.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

As Calo posits, once there is absolutely no privacy in the market, it blows the lid off the whole thing; suddenly, the free market becomes terribly inefficient because goods are not allocated according to price and quality but according to biases, heuristics, and arbitrary tastes.[151] Calo's hypothetical farmer's market, where there is one buyer who knows everything about the many sellers, illustrates the point well.[152] Because the buyer has an information overload about all the sellers and all the products, the buyer relies on heuristics—gut feelings and biases—in order to make a decision. This, in many ways, resembles the reality of consumers' connection to various product markets through advertisement. Consumers are inundated with a deluge of information and advertisements for products in oversaturated markets.

But flip Calo's hypothetical on its head: now there are many buyers but only one seller, like Amazon. Amazon's ability to collect and see all of its buyers' information is integral to this market because when there is only one behemoth of a corporation divvying out everybody's wants and needs, privacy stands in the way of that corporation achieving that goal as efficiently as possible.[153] Calo himself asks whether privacy is conducive to non-market, that is, socialist or noncompetitive, and concludes that such systems are hostile to privacy because a great wealth of data on the population is required to efficiently redistribute resources "to each according to his need."[154] Our own government requires extensive personal information to determine the taxes citizens owe.[155] Thus, Amazon, Facebook, and Google, like the government, must be hostile to consumer privacy in order to be efficient monopolies.

Thus, we have two perspectives from which to view the current behavioral advertising business model. From one perspective, the collection of consumer data allows online platforms—and, relatedly, the marketers to whom the data is sold—to operate efficiently and in a most rational and profit-maximizing way. From the other perspective, the lack of privacy in the market exposes consumers to an information overload that triggers inefficiencies and an inability to act in one's self-interest. The

[151] Calo, *supra* note 11, at 667–68.

[152] *Id.* at 666–67.

[153] *See id.* at 680; Margherita Colangelo & Mariateresa Maggiolino, *Manipulation of Information as Antitrust Infringement*, 26 COLUM. J. EUR. L. 63, 65 (2020) ("[F]irms with a large market may capture and lock-in consumers by providing them with increasingly personalized information and products. Consumers may thus lose interest in other competitors because their needs are constantly analyzed and satisfied by market leaders.").

[154] Calo, *supra* note 11, at 679–80 (quoting Karl Marx, *Critique of the Gotha Programme*, *in* KARL MARX & FREDERICK ENGELS: SELECTED WORKS 13, 14 (1973)).

[155] *Id.* at 680.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

failure of the current antitrust regime is in its focusing on the former, while remaining blind to the latter. It is a watch dog guarding the wrong gate.

In this scenario, it is not just privacy that is the enemy of efficiency, but efficiency that is the enemy of a free and competitive market. Indeed, the objectives of current antitrust and consumer protection laws are not just separate—they are conflicting. This is significant because if our antitrust laws continue to promote efficiency in the new information age while consumer protection laws continue to place privacy in consumers' hands, then there is little room for those laws to simultaneously support the goals of privacy and a free market.[156] This Note's argument is not that competition should be sacrificed in order to protect consumer privacy, but that it is precisely by protecting privacy that we can ensure the survival of competitive market conditions.

One of the main arguments against protecting privacy or restricting advertising from the Law and Economics crowd is the concern that this would disrupt the free flow of information, which would create inefficiency in the market and violate commercial speech protected by the First Amendment.[157] Banning the collection and sale of consumer data may restrict advertisers' free commercial speech because it prevents them from delivering ads, at least more efficiently targeted ads, to consumers.[158] Consumers also supposedly lose out because if advertisers cannot market to consumers more effectively then consumers have less information about products and services upon which to act, rendering the market less efficient.[159]

The issue with this belabored privacy-as-impediment-to-efficiency argument is that it treats privacy as a decidedly one-way street. In an effort to safeguard Coca-Cola's commercial speech, the Law and Economics crowd would have it purchase every trivial detail of my life in order to better market their product to me. In the same respect, should I not be allowed to know everything about Coca-Cola's product, such as, say, its prized secret ingredient in order to make the most efficient and informed consumer decision? Or perhaps there is some credence to the idea of treating consumer data with the same sanctity as trade secrets. At the turn of the millennium, before the meteoric rise of data monopolies, Professor Pamela

[156] *See* Pasquale, *supra* note 8, at 1010.

[157] Cooper, *supra* note 55, at 1140.

[158] *Id.* at 1141–42.

[159] *Id.* at 1143.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

Samuelson made just such an argument.[160] There are three ways, she suggests, in which the interests of trade secrecy and online data privacy overlap: restricting access to information, preventing commercial exploitation, and enforcing minimum standards of commercial morality.[161] It is because of these important goals, which trade secrecy promotes, that allows it to avoid the kind of First Amendment challenges that opponents suggest.[162]

B. Market Manipulation and Behavioral Antitrust

One of the reasons why the current antitrust regime has failed to appreciate the connection between privacy and the free market is that its basic principles rely on the assumption that market actors will behave rationally at least most of the time.[163] It is this same devotion to rationality that blinds Law and Economics to the privacy paradox.[164] On the other hand, there are those within academia who suggest that antitrust should abandon neoclassical economics in favor of behavioral economics.[165] Behavioral economics recognizes that there may be informational or other power imbalances between consumers and large businesses, that consumers do not always behave rationally, and, moreover, that large businesses are capable of using consumer irrationality to their advantage.[166] The Chicago School tolerates monopolies who acquire dominance "legitimately" (i.e. through consumer favor, a superior product, or innovation). However, this fails to capture those instances where a firm acquires and maintains dominance by gaming consumer psychology and irrationality.[167]

---

[160] *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125 (2000).

[161] *Id.* at 1152.

[162] *Id.* at 1157. Samuelson suggests that treating consumer data as trade secrets would avoid the need for a courtroom showdown between First Amendment rights on the one hand and recognizing data privacy as a fundamental civil liberty on the other hand.

[163] Calo, *supra* note 61, at 1000.

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

[165] *See generally* Reeves & Stucke, *supra* note 95.

[166] Max Huffman, Behavioral Exploitation and Antitrust 3–4 (Jan. 2010) (Workshop Draft, NYU Next Generation Antitrust Workshop), http://www.law.nyu.edu/sites/default/files/ECM_PRO_064204.pdf [https://perma.cc/W4HM-B75B]; Calo, *supra* note 61, at 1001 (quoting Jon Hanson & Douglas Kysar, *Taking Behavioralism Seriously: The Problem of Market Manipulation*, 74 N.Y.U. L. REV. 630, 635 (1999) ("Once one accepts that individuals systematically behave in nonrational ways . . . it follows from an economic perspective that others will exploit those tendencies for gain.")).

[167] Colangelo & Maggiolino, *supra* note 153, at 64–65.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

Part II examined how companies may use consumer irrationality, namely through dark patterns, in order to trap users into giving up their privacy. But more importantly, when data is collected, analyzed, and turned into behavioral advertisements it exports the ability to take advantage of consumer irrationality to the larger markets for consumer products and services. This Section explains how behavioral advertising has the possibility of creating anticompetitive and consumer harm beyond just the privacy trade. Behavioral advertising creates a dangerously effective tool for determining a consumer's *individual* idiosyncrasies and irrationalities.[168] This helps firms, in a systematic way, to nullify consumer autonomy in a transaction by approaching a consumer at the exact time and in the exact way that the consumer's deviation from rational self-interest is likely to be most profitable.[169] If our antitrust paradigm is premised on the assumption that rational actors will produce efficient outcomes in a competitive market, then in what sense can we say that an economy reliant upon the systematic undermining of rational behavior is efficient?

Many proponents of the behavioral advertising model suggest that it is no different from advertising in the past, which has always attempted to persuade and influence consumer behavior.[170] To be clear, the marketing industry has always tried to find ways to do more than simply persuade consumers,[171] and the harm to the market writ large has been marginal.[172] During the second industrial revolution, when American households shifted towards consuming mass-produced goods, companies used advertisements as a tool to aid in distribution.[173] But as markets became saturated with goods, companies had to find other ways of remaining viable.[174] When a market is saturated, a company can do one of three things: (1) innovate or improve quality; (2) reduce price; or (3) artificially inflate demand

[168] Calo, *supra* note 61, at 1003.

[169] *Id.* at 1032–33; *id.* at 1018 ("Thus, firms will increasingly be in the position to create suckers, rather than waiting for one to be born.").

[170] Paterson et al., *supra* note 79, at 9; Calo, *supra* note 61, at 1020–21.

[171] Calo, *supra* note 61, at 1020.

[172] *Id.* at 1002; Colangelo & Maggiolino, *supra* note 153, at 70–71.

[173] ERIK LARSON, THE NAKED CONSUMER 18–19 (1992) ("Companies nursed the naïve belief that consumers were rational and would know a good thing when they saw it. To make sure they saw it, companies advertised.").

[174] *Id.* at 20.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

for the good with "unique marketing strategies."[175] Among the unique marketing strategies employed by companies in the first half of the twentieth century, before the FTC Act was enacted, was to brazenly lie and deceive consumers into purchasing a product.[176] Today's marketing craft, however, is vastly more subtle.

Today, behavioral advertising is the magnum opus of what the marketing industry has tried to achieve since the 1910s—namely, the ability of companies to manipulate demand for a product so that they can sustain an oversaturated market without having to innovate, reduce prices, or exit the market. This is because behavioral advertising is fundamentally different from traditional platform-based display advertising, such as in newspaper or television.[177] Whereas the primary goal of the latter is to promote brand awareness, the primary goal of the former is to generate sales.[178] This divergence in advertising goals is based on the ability of companies like Google to analyze consumer data to discover our wants and needs.[179] Dominant platforms can use these insights in combination with dark patterns to further manipulate, influence, and experiment with consumer behavior.[180] As Professor Zephyr Teachout puts it, online platform monopolies "have gone beyond responding to consumer needs to dictating them. All are building systems that suggest what we might want before we've thought of it, prompting desires, not just gratifying them."[181] What made the Cambridge Analytica scandal so infuriating to the public was not only the extent to which Facebook was able to deceive consumers' expectations of privacy, but the extent to which that data could be used to influence electoral and political behavior.[182]

But even more so than this, the fundamental difference in the current behavioral advertising market is its simultaneously systematic, ubiquitous, algorithmic, and machine-driven nature that has the potential to amplify those de minimis harms to

---

[175] Marshall Hargrave, *Market Saturation*, INVESTOPEDIA, https://www.investopedia.com/terms/m/marketsaturation.asp [https://perma.cc/DB5P-KLN3] (last updated May 28, 2021).

[176] LARSON, *supra* note 173, at 20–21.

[177] *See* Newman, *supra* note 89, at 414.

[178] *Id.*

[179] *Id.* at 414–15; Paterson et al., *supra* note 79, at 6–7.

[180] Day & Stemler, *supra* note 68, at 17–19.

[181] ZEPHYR TEACHOUT, BREAK 'EM UP 56 (2020).

[182] *See* Day & Stemler, *supra* note 68, at 21; *see also* Citron & Solove, *supra* note 26, at 47.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

individual consumers into market inequality and failure writ large.[183] The combination of the ability to both analyze and manipulate behavior, thus, has created something of a Schrödinger's consumer. Whereas the advertisements of old may have attempted to influence the behavior of the (relatively) unobserved consumer who was free to behave in an open-ended environment, the ability of companies to observe our behavior, influence it, then observe it again necessarily creates distorted feedback loops that constrict consumers' range of behavioral options until they are pigeon-holed into the perfectly shaped box those companies have made for them.[184]

One result from this arrangement, in terms of antitrust, may be that highly differentiated markets can use behavioral advertising as an implied collusive agreement to fragment the market into consumer cohorts where each differentiated product can exercise a local monopoly on its group of pigeon-holed consumers.[185] Another result could be the de facto segregation of demographics of consumers on the basis of race, gender, or sexual orientation; where virtual redlining and product deserts exist for certain demographics not deemed to be in a company's targeted advertising audience.[186] Thus, the physical geographic component of defining a relevant market in antitrust analysis may become an outdated concept in the face of these business strategies. A consumer's relationship to the wider market is no longer mediated by geography, but by access to an omnipresent platform which deals in information about the market.[187]

The Chicago School is still skeptical of the anticompetitive effects of dealing in undue persuasion; as Judge Easterbrook put it, "[deceptive or manipulative] statements . . . do not curtail output in either the short or long run. They just set the

[183] *See* Calo, *supra* note 61, at 1021, 1024–28.

[184] *See* Paterson et al., *supra* note 79, at 10; *see also* LARSON, *supra* note 173, at 15 ("We don't see how the marketers have eroded our civil liberties; how by invoking the great god Efficiency they created an electronic caste system in which all of us reside and that reinforces class stereotypes and fosters a subtle new brand of discrimination . . . .").

[185] *See* Lola Esteban & Jose Hernandez, *Strategic Targeted Advertising and Market Fragmentation*, 12 ECON. BULL. 1 (2007); Lynne Pepall & Joseph Reiff, *The "Veblen" Effect, Targeted Advertising and Consumer Welfare*, 145 ECON. LETTERS 218 (2016).

[186] Jon M. Garon, *Dysregulating the Media: Digital Redlining, Privacy Erosion, and the Unintentional Deregulation of American Media*, 73 ME. L. REV. 45, 73–74 (2020); *see also* James A. Allen, *The Color of Algorithms: An Analysis and Proposed Research Agenda for Deterring Algorithmic Redlining*, 46 FORDHAM URB. L.J. 219 (2019) (making the case that algorithms promote racial stereotypes because they are fed with data that is itself the product of historical discrimination).

[187] Calo, *supra* note 61, at 1003.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

stage for competition in a different venue: the advertising market."[188] Thorstein Veblen, an economic theorist from the turn of the century, put it another way: "Each [business] must advertise, chiefly because the others do."[189] What Judge Easterbrook may have failed to realize is that when the venue for competition is advertising, businesses divert their competitive efforts away from improving the quality and price of their product.[190] Taken to an extreme, the ability of firms to control information and manipulate consumer behavior in a highly differentiated or fragmented market may reach to such an extent that firms may find no need to actually create or market anything of productive value at all. Firms could create speculative value out of a peppercorn and convince their niche microcosms of consumers to buy in for the sole sake of its being apparently valuable.[191] When you give the market lemons, convince them it's lemonade.

One handy tool in the behavioral advertising arsenal that helps firms achieve this outcome is taking advantage of consumers' irrational attribution of value in acquiring a sense of belonging and social status in a given social or interest group.[192] The effect can be self-reinforcing, as the firm need only convince a few members of

[188] Colangelo & Maggiolino, *supra* note 153, at 70.

[189] THORSTEIN VEBLEN, THE THEORY OF BUSINESS ENTERPRISE 58 (1904).

[190] *Id.*; *see also* Colangelo & Maggiolino, *supra* note 153, at 68 ("This may be the case if, in the short-term, the practice of spreading false and disparaging information is significantly less expensive than any investment in improving the quality of product offerings."); LARSON, *supra* note 173, at 15 ("All this corporate probing, moreover, has produced a business culture that shies from true innovation and pays more attention to manipulating our needs, values, and shopping behavior than to giving us a better product. This dependence has grown so pervasive that it has crimped the national imagination . . . .").

[191] These types of commodities are aptly named "Veblen Goods." *See* James Chen, *Veblen Good*, INVESTOPEDIA, https://www.investopedia.com/terms/v/veblen-good.asp [https://perma.cc/X5G2-CBGW] (last updated Nov. 30, 2020); Pepall & Reiff, *supra* note 173, at 218 ("However, unlike in Veblen's era, this effect is no longer restricted to luxury goods."). The current craze over Non-Fungible Tokens (NFTs), which may or may not be only a passing fad, is nevertheless emblematic of this larger issue. *See* Luke Savage, *NFTs Are, Quite Simply, Bullshit*, JACOBIN (Jan. 26, 2022), https://jacobinmag.com/2022/01/nfts-fallon-paris-hilton-bored-ape-digital-imagery-commodification [https://perma.cc/D6C2-9H7G] ("Like cryptocurrency, it's hard to make a case for their actual use value and, like the very dumbest Silicon Valley startups and multilevel marketing scams, they're best understood as speculative investments in which a privileged few can wring money from something of no redeeming social benefit."). The only thing that gives these peppercorns more value is convincing more consumers, and even sellers, that they have value; thus, "'[i]ncreased adoption means exponentially increased value and utility.'" Robert Farrington, *Why Big Brands Are Spending Millions on NFTs*, FORBES (Dec. 25, 2021, 10:30 AM), https://www.forbes.com/sites/robertfarrington/2021/12/25/why-big-brands-are-spending-millions-on-nfts/?sh=11e9641d6117 [https://perma.cc/AR8H-XMNJ].

[192] *See* Pepall & Reiff, *supra* note 185, at 218–19.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

the social group to purchase the product—and perhaps to conveniently display it to their peers via social media—in order to propagate the perception that the product is needed to belong to the group.[193] Although consumers find some value in achieving social status, in reality they end up economically worse-off because output will decrease and price will increase.[194] To be sure, "[t]he market tolerates a measure of this behavior."[195] There is nothing wrong with differentiated products that appeal to different consumers' tastes. However, when replicated across more and more product markets that rely on behavioral advertising to reach subsets of consumers, "the unfettered personalization of transactions will balkanize markets, splintering each market into smaller markets of the like-minded."[196] By all means, let a product differentiate itself in a market, but let it do so by the measure of its quality, design, uniqueness, and innovation, and not by the measure of its ability to target and manipulate subsets of consumers.

IV. PROPOSAL

A few things should be clear about the behavioral advertising business model from the foregoing discussion: (1) it gives dominant firms an incentive to invade privacy, and to manipulate consumers' behavior into surrendering privacy and spending more time online; (2) consumers are unable to overcome cognitive biases and choose non-privacy-invasive internet services, despite having access to platforms' information collection practices; (3) it creates entry barriers for non-privacy-invasive business models; and (4) it allows companies to take advantage of consumer irrationality to manipulate market outcomes. Any regulatory proposal that seeks to safeguard consumer privacy must address each of these interrelated problems.

Notice and choice, and other regulatory regimes premised on the self-management of personal data, such as the General Data Protection Regulation ("GDPR"), are inadequate because of their failure to take into account consumer irrationality in the face of online platforms' immense market power.[197] As an

[193] *Id.*

[194] *Id.* at 219.

[195] Calo, *supra* note 11, at 667.

[196] *Id.*

[197] Solove, *supra* note 41, at 33.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

example, one of the GDPR's privacy regulation principles, data portability,[198] demonstrates why antitrust considerations must factor into privacy regulation. Essentially, data portability is the right to request that a company transfer all of one's collected personal data to another company.[199] Data portability makes it easier to switch to a competitor that offers better data privacy and security because data can be easily transferred from the other platform, lowering entry barriers and network effects by not making potential customers rebuild their network.[200]

However, data portability is a toothless privacy protection if no competitors actually exist to switch to.[201] Zuckerberg himself is advocating for the FTC to adopt data portability, not out of the goodness of his heart, but because he knows that superficial changes like this operate to forestall or mask more meaningful change in antitrust law.[202] This is why preventing anticompetitive acquisitions, like that between Facebook and WhatsApp, is necessary for data portability to work because it prevents the market giants from immediately buying out potential competitors.

Even then, data portability would still fail to protect privacy because, as discussed in Section II.A, the ability of data collecting firms to generate revenue with behavioral advertising makes other business models unprofitable. Consumers have already demonstrated their unwillingness to pay for their privacy, and there is no reason to think data portability would change that calculus. It is precisely this kind of consumer behavior that also makes the approach to privacy protection through breaking up these data monopolies counterproductive. If consumers are motivated by convenience and instant gratification, rather than rationally weighing the value of their privacy, then consumer preference even in a competitive market is hardly likely to drive privacy protection.[203] The simple, but counterintuitive, truth is that consumers cannot, and thus should not, manage their own privacy because

[198] Directive 2016/679, art. 20, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC, 2016 O.J. (L 119) [hereinafter General Data Protection Regulation].

[199] *Id.*

[200] Harbour & Koslov, *supra* note 8, at 796.

[201] Mark Emem, *Facebook's Latest Scheme to Kill Competition: Data Portability*, CCN (Aug. 23, 2020, 3:37 PM), https://www.ccn.com/facebooks-scheme-kill-competition-data-portability/ [https://perma.cc/AN9F-YL2N].

[202] *Id.*

[203] MARTHEWS & TUCKER, *supra* note 114.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

consumers' decisions do not only affect their own privacy but facilitate the structural dominance and pervasive surveillance of a ubiquitous behavioral advertising industry for everybody.[204] Privacy is not a private good that can be supplied by a private market, but a public good that must be provided by the public sphere.[205]

Solove suggests that even if we were to magically cure consumers' irrationality, self-management would still fail.[206] This is, in part, because even if consumers fully understood the implications of data collection and behavioral manipulation, it is impossible to read every privacy policy and select different privacy settings (which may or may not exist at all) across thousands of websites.[207] Any real privacy protection must be comprehensive and set a uniform industry-wide standard that consumers can rely on without having to manage it themselves.

The proposal, then, must be to ban data collection and/or behavioral advertising as a business model and allow the internet to reorganize itself competitively by offering consumers an array of options that do not involve surveillance as the primary means of generating revenue.[208] We might think of a behavioral advertising ban as a kind of norm enforcing default rule, recalling the earlier discussion of default rules.[209] A norm enforcing default alters the behavior of contracting parties with reference to a substantive value, in this case privacy.[210] As such, a ban becomes a uniform provision in privacy policies that consumers can come to expect and rely upon.

---

[204] *See* Paterson et al., *supra* note 79, at 5 ("[T]he impact of individual decisions about data sharing on the collective interests of consumer means that there is a good case for treating algorithmically targeted advertising systematically, rather than leaving the responsibility to affected individuals."); *see also* Janger & Schwartz, *supra* note 31, at 1251.

[205] *See* Janger & Schwartz, *supra* note 31, at 1252.

[206] *See* Solove, *supra* note 41, at 42–43.

[207] *Id.* at 45.

[208] *See* K. Sabeel Rahman & Zephyr Teachout, *From Private Bads to Public Goods: Adapting Public Utility Regulation for Informational Infrastructure*, KNIGHT FIRST AMEND. INST. (Feb. 4, 2020), https://knightcolumbia.org/content/from-private-bads-to-public-goods-adapting-public-utility-regulation-for-informational-infrastructure [https://perma.cc/6XJM-VA24] ("Banning targeted ads falls squarely in the tradition of these regulatory techniques. As with nondiscrimination and common carriage, the ban would place limits on the kinds of practices legally available to information platforms. Like fair pricing requirements, the ban would alter the revenue-generating strategy of the firms themselves.").

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

[210] Janger & Schwartz, *supra* note 31, at 1245.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

A ban first and foremost addresses the issue of consumers irrationally giving up their privacy to online platforms. It not only avoids the need for consumers to behave superrationally, but it also eliminates the primary profit incentive of platforms to use dark patterns, toxic content, and manipulation in order to get consumers to give up their privacy and spend more of their attention on the platform. It also addresses the competitive problem of entry barriers for start-ups who seek to use a business model that values consumer privacy.

Secondly, a ban would also solve the consumer protection and competition problems posed by the ability of firms to use behavioral advertisements to systematically manipulate consumers to behave irrationally. As Calo,[211] Citron, and Solove[212] point out, addressing these kinds of manipulative harms, similar to how the FTC addresses deceptive practices, is likely not to be helpful, as manipulation is difficult to prove, and the harm to consumers on an individual basis is marginal. Relatedly, attempts to characterize manipulation through behavioral advertising as an antitrust violation has been met with difficulty and skepticism by courts.[213] This is usually the case because, when the market's mechanisms operate properly, consumers that recognize a firm's deception will generally be able to leave that firm for another firm that does not engage in such harmful practices.[214] However, unlike deception, consumers cannot easily tell when they have been manipulated.[215] Thus, this leads to a wider failure of the market mechanisms by which a manipulative firm would not have been able to sustain market dominance.[216] In such instances of market failure, Colangelo and Maggiolino suggest that antitrust is not the proper avenue to address the issue, but rather through legislation that targets the manipulative conduct capable of causing the market failure.[217]

One way to achieve a behavioral advertising ban is through the promulgation of regulations by the FTC under its "unfair competition" authority.[218] There are also other tools in the antimonopoly toolbox, beyond antitrust law, that can achieve a

[211] *See* Calo, *supra* note 61, at 1002.

[212] Citron & Solove, *supra* note 26, at 48.

[213] *See* Colangelo & Maggiolino, *supra* note 153, at 70–71.

[214] *Id.* at 72–73.

[215] *Id.* at 73.

[216] *See id.*

[217] *Id.*

[218] Rothchild, *supra* note 2, at 637.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu

similar outcome, such as regulating platforms like Facebook and Google as public utilities.[219] This is more beneficial than a strictly antitrust approach that breaks up monopolies. As Rahman and Teachout admit, "we would still see a value in some degree of consolidation in key communications tools."[220] Thus, we could still benefit from the efficiency of a free and consolidated search engine, but without the perverse economic incentives or surveillance. After all, "antimonopoly is more than antitrust."[221]

These public utilities can be funded through a variety of means, such as taxes, subscription fees, regular display advertising, or a combination of all three.[222] Display advertising, which does not rely on surveillance and data collection, has always been relied upon by traditional information infrastructure (TV, newspapers, radio) to subsidize revenue, and there is no reason why the internet cannot, or should not, follow suit.[223] Banning behavioral advertising does not mean fundamentally changing the way we interact or receive information online. At its core, the only change is in the underlying base of revenue.

V. CONCLUSION

The current notice and choice framework fails to adequately address consumer privacy concerns online or to properly moderate the privacy trade. Part of its shortcomings is due to the irrational behaviors of consumers acting on cognitive biases and the manipulation of consumer behavior by dominant platforms to erode privacy and capture attention. The other part of its shortcomings is due to its failure to consider the effects of the behavioral advertising business model on the competitive structure of the internet economy. Data collection by dominant platforms creates a steep entry barrier for other competitors, thus creating a dearth of options for consumers to exercise their privacy preferences. Ultimately, protecting consumer privacy means eliminating the very thing that undermines it. Banning the behavioral advertising business model would not dissolve the internet as we know it—it would only eliminate the revenue model that has led to so many societal ills. Banning behavioral advertising, thus, is the only sensible regulatory framework for protecting both consumer privacy and economic freedom.

---

[219] Rahman & Teachout, *supra* note 208.

[220] *Id.*

[221] *The New Brandeis Movement*, *supra* note 147, at 1.

[222] Rahman & Teachout, *supra* note 208.

[223] *See id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.871
http://lawreview.law.pitt.edu