Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy

Christopher W. Savage*

22 STAN. TECH. L. REV. 95 (2019)

ABSTRACT

Privacy interests arise from relationships of trust: people share information with those they trust and conceal things from those they don't. Trust grows when it is respected and diminishes if it is betrayed. Firms in the online ecosystem need consumers to trust them, so the consumers keep coming online, being surveilled, viewing ads, and buying things. But those same entities make money by exploiting consumer trust—using the information they gain to develop individualized profiles that facilitate advertising that gets people to buy things they may not really want or need, at individualized rather than generally available prices. Trust and, thus, privacy, is therefore best viewed as a common-pool resource for the online ecosystem to manage, not as a commodity exchanged in a market between consumers and sellers. The common-pool resource model explains why online entities have incomprehensible privacy policies, why they accept regulation by the Federal Trade Commission, and why they recognize the seriousness of data breaches even as they reject any obligation to compensate consumers when a breach occurs. This model also clarifies the nature of the ongoing economic and political conflict between consumers and online entities about pervasive surveillance and the use of targeted ads. Market-based models, by contrast, do not fit these realities and, as a result, there is no reason to think that "market forces" will optimally equilibrate consumer and seller interests. Some modest regulatory correctives are therefore advisable.

* George Washington University Law School, Professorial Lecturer in Law; Columbus School of Law (Catholic University), Lecturer in Law; Partner, Davis, Wright Tremaine, LLP. J.D., Harvard Law School (1980); B.A., Harvard College (1977). The views expressed here are the author's own, and do not necessarily reflect those of any of the institutions with which he is affiliated or any of the clients of his law firm.

TABLE OF CONTENTS

I. INTRODUCTION

Over the last twenty-five years, the internet has transformed our economy, politics, and culture.[1] It enables the creation, recording, and analysis of unfathomable amounts of information about everything we do, both online and offline. When transformative new technologies arise, they quickly permeate the culture and the

1. This article uses the term "internet" as shorthand for the internet itself—the world wide web, Facebook, Google, YouTube, Twitter, eBay—as well as the communications and computing technology that supports it and enables access to it, including smartphones, tablets, laptops, etc.

economy, creating new conflicts and problems to which existing legal doctrines do not readily apply. The law then plays catch-up to address the issues the new technology creates.[2] The law of information privacy is still catching up with the consumer surveillance economy the internet has created.

John Maynard Keynes once said, "Economics is the science of thinking in terms of models joined to the art of choosing models which are relevant to the contemporary world."[3] The thesis of this article is that much of the legal and policy debate surrounding online consumer privacy has been based on the wrong economic model. The standard approach uses the market as the institutional framework within which to understand privacy policy. The idea is that consumers are (or could be or should be) aware of what information is collected while they are online and what is done with it, and that they do, or can, or should, choose their online activities based on that awareness. This vision of informed, empowered, decisive consumers fits with the "notice-and-choice" model of privacy embodied in the Fair Information Practices from the 1970s.[4] It also facilitates an economic analysis under which consumer choices supposedly reveal something about the privacy people want, and within which online entities compete by offering greater or lesser privacy protections.

The market model provides benefits on two levels. First, it is extremely well-understood. The basic idea traces back at least to Adam Smith, and the familiar image of supply and demand curves intersecting at a stable equilibrium level of price and quantity dates to more than 150 years ago, with the modern presentation established by Alfred Marshall in 1890.[5] Standard microeconomics is, so to speak, in the air, and policymakers, businesspeople and consumers alike naturally see the world through its lens.[6] Second, when market forces are working well, they pro-

2. *See* David L. Markell & Robert L. Glicksman, *Dynamic Governance in Theory and Application Part I*, 58 ARIZ. L. REV. 563, 575-78 (2016). *See also* CARLOTA PEREZ, TECHNOLOGICAL REVOLUTIONS AND FINANCIAL CAPITAL: THE DYNAMICS OF BUBBLES AND GOLDEN AGES 23-24 (2002) (revolutionary new technologies generate "changes in the regulatory framework affecting all markets and economic activities"); *id.* at 114-26, 128-32.

3. Letter from J.M. Keynes to Roy Harrod (July 4, 1938), *in* THE COLLECTED INTERWAR CORRESPONDENCE OF ROY HARROD (Daniele Besomi ed., 2003), https://perma.cc/L7MV-WXXW (reprinted as Letter 787).

4. *See infra* Parts II.A and II.D.

5. Thomas M. Humphrey, *Marshallian Cross Diagrams and Their Uses before Alfred Marshall,* 78 FED. RES. BANK RICHMOND ECON. REV. 3, 3-4 (1992).

6. As Keynes said, "Practical men, who believe themselves to be quite exempt from any intellectual influences, are usually the slaves of some defunct economist." JOHN MAYNARD KEYNES,

duce more than an equilibrium; they produce an allocation of resources that is optimal—the desires and needs of consumers are balanced, at least presumptively fairly, against the interests of producers.[7]

But problems with the market model, both real-world and analytical, are well-known. In addition to high transaction costs, externalities, and information asymmetries, the idea that consumers can make meaningful choices about online privacy is practically a poster child for the behavioral economic critique of standard microeconomics. People aren't good at bargaining over complex, contingent, or uncertain future costs and benefits of the sort arising from online surveillance; no such bargaining occurs in fact; and it's not clear why rights in information arising from interactions between an individual and an online entity belong to the individual (to be bargained over) rather than the entity (to be exploited at will).

In fact, the misfit of the market model is more fundamental than obvious market failures and bounded rationality. Privacy arises from relationships of trust. People share information with those they trust, and conceal things, if they can, from those they do not. If trust proves warranted, it grows; if it is betrayed, it diminishes. These are not market transactions at all; they are social and psychological phenomena. Furthermore, online entities want people to trust them so they will keep coming online, sharing information, being surveilled, viewing ads, and buying things. That process necessarily entails making use of consumers' trust—by selling information about them (directly or indirectly) to third parties, who use it to try to get people to buy things they may not really want or need, at individualized rather than generally available competitive prices. Consumer trust, therefore—with its associated expectations of privacy—is best viewed as a common resource that online entities work simultaneously to use and to preserve. If they can sufficiently limit the degree to which their actions erode trust, they can continue to mine it. If not, the entire consumer-facing online business model is at risk. Online entities are thus not competing in a market to provide consumers with an optimal level of privacy; they are cooperating in an effort to ensure that the level of consumer trust doesn't sink so low that people stop coming online. This situation does not describe a market. It describes a commons, in which consumer trust is the common-pool resource.

Seeing the world through the wrong model has consequences. In a functioning market, producers and consumers can rely on the forces of competition to bring

THE GENERAL THEORY OF EMPLOYMENT, INTEREST AND MONEY 258 (Kindle ed. 2009) (1936).

7. *See infra* Part III.A.

prices, product features and the terms of sale more or less into alignment with what consumers, considered as a whole, want. So, producers who assume they are operating in a market, but do not receive economic pushback from consumers, will assume that consumers find the prices, features, and terms of service of their offerings generally acceptable. For their part, consumers who assume they are operating in a market will believe that the goods and services on offer reflect producers' efforts to provide what consumers as a whole actually want. And policymakers who believe they are seeing a market in action will assume that that kind of equilibration is occurring, miss signals when something is amiss, and reach for the wrong regulatory toolkit to deal with any problems they do perceive.[8]

Unlike a market model, the commons model explains why online entities have obscure and even incomprehensible privacy policies; it explains the industry's acceptance of regulation by the Federal Trade Commission (FTC) based on those policies; and it explains the industry's recognition of the seriousness of consumer data breaches even as it strenuously fights the idea that breaches cause compensable harm. It also clarifies the nature of the ongoing economic (and political) conflict between consumers and online entities about pervasive surveillance and the use of targeted ads. Market-based models, by contrast, provide (at best) a Procrustean fit to these and other realities of online consumer privacy.[9]

The remainder of this Article is organized as follows. Part II summarizes the history of the "notice-and-choice" information privacy framework; sketches some of the key features of the online surveillance economy; outlines the standard economic analysis of consumer privacy issues; and presents the standard economic challenges to it. Part III explains how a commons differs from a market, and describes the ambient online trust commons—including two unique features that distinguish it from a typical natural resource commons. Part IV explores some of the implications of looking at online consumer privacy issues using the model of the ambient trust commons. Part V offers some concluding observations.

8. As Hayek observed, a key function of markets is to both create and disseminate critical information about products' prices and characteristics and the resources used in their production. F.A. Hayek, *The Uses of Knowledge in Society*, 35 AM. ECON. REV. 519, 524-28 (1945). But when markets aren't working, the critical information will be distorted or unavailable—a situation made even worse when policymakers, producers, and consumers believe markets *are* functioning and *are* delivering accurate information.

9. *Cf.* DR. SEUSS, ONE FISH, TWO FISH, RED FISH, BLUE FISH 20-21 (1960).

II. THE STANDARD MODEL

A. Information Privacy before the Internet

Modern information privacy law arose in the late 1960s as scholars and policymakers began to worry about computerized databases used to track government benefits (such as Social Security payments) or, in the private sector, to make decisions such as whether to extend credit.[10] Before computerized databases, everyone benefitted from "security by obscurity"—information about everyone was theoretically available in the records and knowledge of individual friends, acquaintances, or merchants, but those facts were not readily accessible.[11] As it became easier to put lots of facts together into databases, policymakers became concerned.

In response, Congress enacted statutes addressing the collection and use of information in specific contexts: access to credit, government records, educational records, etc.—giving special status to information deemed particularly worthy of protection.[12] Governmental and quasi-governmental groups developed principles thought to usefully apply to the collection and use of personal information, whether especially sensitive or not. The seminal effort was the "Fair Information Practices," or FIPs, developed by a committee working under the Department of Health, Education and Welfare, published in 1973.[13] The FIPs envision that people know what information is being collected and how it will be used, ban its use for other purposes

10. The key text from this period is ALAN WESTIN, PRIVACY AND FREEDOM (1967), especially (for our purposes) ch. 7, "The Revolution in Information Collection and Processing: Data Surveillance," and ch. 12, "Putting All the Facts Together."

11. *See, e.g.*, Kuang-Wen Wu et al., *The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust*, 28 COMPUTERS IN HUM. BEHAV. 879, 890 (2012) [hereinafter *Effect of Online Privacy Policies*] ("In the paper-and-ink-world, the sheer physical effort of collecting, archiving, and analyzing such data acts as a deterrent which helps to protect privacy to a certain extent."); Jesper M. Johansson & Roger Grimes, *The Great Debate: Security by Obscurity*, TECHNET (Sept. 27, 2016), https://perma.cc/CT8Z-DFP5. The "right to be forgotten" reflects an effort to restore some aspects of pre-internet obscurity. *See generally* Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L.J. 981 (2018).

12. *E.g.*, 5 U.S.C. § 552(a) (2017) (restraining the use and disclosure of information in a governmental "system of records"); 15 U.S.C. § 1681 (2017) (ensuring people have access to their credit reports and limiting dissemination); 20 U.S.C. § 1232g (2017) (restraining disclosure of educational records). As time went on, additional sectors were addressed by statute on an *ad hoc* basis, including cable television viewing, 47 U.S.C. § 551 (protecting cable viewing habits); video rentals, 18 U.S.C. § 2710 (protecting records of video or similar rentals); and health care information, Health Insurance Portability & Accountability Act (HIPAA), P.L. 104-191, § 264(c).

13. SEC'Y'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEP'T. OF HEALTH, EDUC. AND WELFARE, DHEW PUB. NO. (OS)73-94, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS xxiii (1973).

without consent, require an opportunity to correct errors, and oblige the organization with the information to safeguard it. Similar principles were adopted by the Organization for Economic Cooperation and Development (OECD) in 1980, updated in 2013.[14]

These principles do not suggest that consumers can refuse to provide information, such as credit history when applying for a loan, or medical history when applying for life insurance. Data collection is inevitable. At a minimum, a merchant will need payment information from the customer and a delivery address (physical or virtual) for the product. Today, for a consumer to view a website, the servers hosting the site must know the IP address, browser type, and other metadata regarding the computer and browser making the request. But in most cases, there is no legal compulsion to retain this information, and online sellers and websites could delete it, or much of it, promptly after each transaction was completed. Participating in the economy means that consumers necessarily supply, and merchants necessarily collect, a great deal of information, but how much of it the merchant chooses to retain, and what she does with it (beyond fulfilling the particular transaction) are matters of the merchant's choice. The FIPs and OECD principles focus on ensuring that consumers are aware of what information is being collected and retained, and on limiting its use for unrelated purposes.

B. The Consumer Internet

While general privacy principles were being developed, the internet was evolving from an obscure government research and communications tool into a mass consumer phenomenon. In the 1990s, the Clinton administration was keenly aware of the potential benefits of modern communications and computer technology. This was a period of techno-optimism, with the administration promoting the "National Information Infrastructure," sometimes called the "Information Superhighway."[15] The Telecommunications Act of 1996,[16] passed during this period, aided the development of the internet in several ways. One new provision, 47 U.S.C. § 230, declared that the "policy of the United States" was to "preserve the vibrant

14. OECD, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), https://perma.cc/UW7G-DD3V; OECD, PRIVACY GUIDELINES (2013), https://perma.cc/3X73-TY3C.

15. *See generally* Jonathan D. Blake & Lee J. Tiedrich, *The National Information Infrastructure Initiative and the Emergence of the Electronic Superhighway,* 46 FED. COMM. L.J. 397 (1994).

16. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified at scattered sections of 47 U.S.C.)

and competitive free market that presently exists for the Internet . . . unfettered by Federal or State regulation."[17] Another new provision, Section 706 of the 1996 Act (later codified at 47 U.S.C. § 1302), directed the Federal Communications Commission (FCC) and the states to "encourage the deployment of advanced telecommunications capability," which was read to include broadband (i.e., high bit-rate) internet access.[18]

The 1996 Act also outlawed monopolies for landline local telephone service[19]—just as consumer demand for internet access was exploding. Access at that time was mainly via dial-up connections to local Internet Service Providers (ISPs). Many of the new local carriers chose to focus on providing ISPs the telephone connections they needed. The result was thousands of dial-up ISPs a mere phone call away, enabling robust competition that helped expand mass market internet access.[20] The success of dial-up demonstrated strong and growing demand for internet access, which provided a business justification for cable operators and others to make the investments needed to provide broadband.[21]

C. The Surveillance Economy

Online activities, including browsing, posting to social media sites, and reading and writing emails on services such as Google or Yahoo, are subject to pervasive and detailed surveillance. In addition to tracking by websites, online services, and

17. 47 U.S.C. § 230(b)(2).

18. *E.g.*, Second Report, *In re* Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, 15 FCC Rcd. 20913 ¶¶ 2, 28-61 (2000) (discussing technologies used to provide broadband internet access). For a summary of FCC policies that helped the internet develop, see J. Oxman, *The FCC and the Unregulation of the Internet* (FCC Office of Plans and Policy, Working Paper No. 31, July 1999), https://perma.cc/6TXE-742H.

19. 47 U.S.C. § 253(a).

20. *See, e.g.*, Report to Congress, *In re* Federal-State Joint Board on Universal Service, 13 FCC Rcd. 11501 ¶ 81 (1998).

21. In 2002, the FCC ruled that broadband ISPs need not provide competitors with transport between end users and competitor locations—that is, they didn't have to provide the broadband equivalent of dial-up calls to competing ISPs. Declaratory Ruling and Notice of Proposed Rulemaking, *In re* Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities; Internet Over Cable Declaratory Ruling; Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities, 17 FCC Rcd. 4798 ¶ 43 (2002). Without access to broadband connections, competitive ISPs largely faded away, so that today only entities that own local transport networks—cable companies, telephone companies, and wireless companies—can effectively provide mass-market broadband internet access.

associated advertising networks, mobile devices track people's locations and activities with great precision.[22] Biometric sensors in billboards permit advertisers to choose which ad to display based on the apparent age and gender of those nearby.[23] Firms such as Equifax, Experian, Acxiom and ChoicePoint ("data brokers") assemble and maintain detailed profiles on essentially all adult Americans based on both "real life" and online activities. These profiles are then sold to marketers.[24]

Privacy law and policy distinguish between especially sensitive information, such as health data or financial account information, and more pedestrian data about what websites people visit, or whose posts they respond to on social media.[25] It is not clear, however, that this distinction makes a difference with respect to advertising-driven online commercial activity. Modern data mining and predictive profiling techniques permit marketers to identify consumers well enough to target ads with at times uncanny precision, relying mainly or entirely on boring, non-sensitive data.[26] Data mining entails using sophisticated computer programs to analyze large collections of data to find patterns that a human researcher could not identify.[27] Predictive profiling starts with a deep analysis of everything an advertiser knows about existing purchasers and uses that information to decide what products to offer, and at what prices, to other individuals whose profiles "look like" those of previous customers.[28] These targeted ads are designed to interest individual consumers, and can include offers at specific prices calculated to be just below what

22. *See, e.g.*, Carpenter v. United States, 585 U.S. ___, 138 S. Ct. 2206, 2220 (2018) (noting location tracking as a result of the normal operation of ubiquitous mobile phones).

23. *See, e.g.*, FTC, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (Oct. 2012), https://perma.cc/9W5X-MDLF.

24. *See generally* FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY [hereinafter DATA BROKERS] (May 2014), https://perma.cc/MH7F-X77R; Chris J. Hoofnagle, *et al., Behavioral Advertising: The Offer You Cannot Refuse,* 6 HARV. L. & POL'Y REV. 273 (2012) [hereinafter *Offer You Cannot Refuse*].

25. *See, e.g.*, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (Feb. 2009) [hereinafter SELF-REGULATORY PRINCIPLES], https://perma.cc/56VL-8YE8.

26. *See* Nathan Newman, *Search, Antitrust, and the Economics of the Control of User Data,* 31 YALE J. ON REG. 401 (2014) [hereinafter *Control of User Data*]; *see also* Jan Whittington & Chris Jay Hoofnagle, *Social Networks and the Law: Unpacking Privacy's Price,* 90 N.C.L. REV. 1327 (2012) [hereinafter *Unpacking Privacy's Price*].

27. Ryan Calo, *Digital Market Manipulation,* 82 GEO. WASH. L. REV. 995, 1008-09, 1011 (2014) [hereinafter *Digital Market Manipulation*].

28. David C. Vladeck, Response, *Digital Marketing, Consumer Protection, and the First Amendment: A Brief Reply to Professor Ryan Calo,* 82 GEO. WASH. L. REV. ARGUENDO 156, 157 (2014) (marketers "leverage the power of 'big data' to prepare highly personalized profiles on consumers"); Joshua A.T. Fairfield & Christian Engel, *Privacy as a Public Good,* 65 DUKE L.J. 385, 389 (2016) [hereinafter *Privacy as a Public Good*].

each individual consumer is willing to pay.[29] This system works: targeted ads produce many times the "click-through rate" of untargeted ads, and have an overall "conversion rate" (clicked-on ads leading to sales) more than twice as high as untargeted ads.[30]

At the same time, the success rate for online ads is abysmal—viewers click on less than 1% of ads displayed, and click-through rates even for ads on highly targeted services like Facebook and Twitter are in the range of 1 to 3%.[31] Online advertising remains viable due to its sheer scale. Google AdWords has been reported to serve nearly 30 billion ads each day.[32] This combination—a vast number of ads with an overall very low success rate—means that the concern is not that people are somehow in thrall to ads. To the contrary, by a wide margin, people mostly ignore them.[33] The issues arise from the statistical, cumulative effect of billions of ads, not any one ad considered in isolation.[34]

With some narrow exceptions—such as restrictions on collecting information from children[35]—federal law does not restrict tracking and storing detailed information about online activities, combining that information with data about offline

29. *Control of User Data*, *supra* note 26, at 443 ("Advertisers are able to exploit the fact that different people have different maximum prices they are willing to pay, the so-called 'pain point' after which they will not buy the product.").

30. Howard Beales, *The Value of Behavioral Targeting*, NETWORK ADVERTISING INITIATIVE (2010) (citing, e.g., Jun Yan, et al., *How Much Can Behavioral Targeting Help Online Advertising,* WWW 2009 MADRID! (2009)), https://perma.cc/54M4-3KLR. Reportedly, the click-through rates for targeted ads were nearly seven times as high as for more generic ads. *See also* Austen Hufford, *Online Ads that Follow You Are Getting New Scrutiny,* THE WALL STREET J. (June 18, 2018), https://perma.cc/Q5CJ-QWYV (stating highly personalized ads have three times the click-through rate of non-personalized ads).

31. Dave Chaffey, *Average Display Advertising Click-Through Rates,* SMART INSIGHTS (Mar. 14, 2018), https://perma.cc/AT7X-U9QE. *See also* Hufford, *supra* note 30 (stating generic ads have a click-through rate of only 0.12%, and personalized ads have a rate of only 0.36%).

32. Larry Kim, *How Many Ads Does Google Serve in a Day?* (Nov. 2, 2012), https://perma.cc/4RUE-CF7L.

33. This provides a corrective to claims that modern advertising somehow controls people's actions or values. *E.g.*, Yoav Hammer, *Expressions Which Preclude Rational Processing: The Case for Regulating Non-Informational Advertisements,* 27 WHITTIER L. REV. 435, 457-51, 466-67 (2005) [hereinafter *Regulating Non-Informational Advertisements*].

34. Woodrow Hartzog & Daniel J. Solove, *The Scope of Potential of FTC Data Protection,* 83 GEO. WASH. L. REV. 2230, 2283 (2015) [hereinafter *Potential FTC Data Protection*] (harms from privacy and data security violations "are often quite dispersed and have more of a dispersed societal impact rather than a concentrated impact on any one individual"). *See also* A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements,* 2015 U. ILL. L. REV. 1713 (2015) (comparing small privacy violations to environmental toxins, which increase risk of harm rather than creating one-to-one impacts). In the online ad context, while most people can resist ads some of the time, and some people can resist ads most of the time, probably no one can resist all ads, all of the time. *See infra* note 230.

35. Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-05 (2018); 16

activities, creating detailed profiles based on mining the combined dataset, and then developing and displaying targeted ads based on the profiles.[36] These practices thus continue to grow and, indeed, form the economic foundation of the consumer-facing, advertising-supported internet ecosystem.[37]

Detailed information about individual consumers is valuable to marketers, but neither they nor online entities have any direct economic motivation to respect privacy. To the contrary, their economic interest is to surveil users as much as possible and obtain as much economic benefit as possible from the information thus gleaned. At some point, surveillance might reach a point of diminishing returns, but given the exceedingly low cost of surveillance, the limiting factor will probably be when surveillance becomes so excessive that it is impossible to conceal, making people nervous enough to cut back on their online activities. The motivation of online entities is to surveil their users, in effect, as much as those users can stand.

D. The FTC and Online Privacy

As the internet was becoming a mass consumer phenomenon, and as online entities began to appreciate the value of tracking and making use of information about consumers, the FTC began worrying about online privacy.[38] Privacy in the commercial context meant some version of the FIPs, and a bedrock principle of the FIPs is *notice.* Any claim that privacy interests were being protected would be untenable if consumers were not even aware that information about them was being gathered and used. The FTC, therefore, began expressing concern that many websites had no disclosures regarding what information they were collecting and what they were doing with it.[39]

C.F.R. § 312 (2018) (FTC rules implementing COPPA).

36. *Potential FTC Data Protection, supra* note 34, at 2267 ("There is no federal law that regulates much of online commerce."). There is a smattering of recent exceptions at the state level. *E.g.*, 2017 Vt. Laws 171 (imposing reporting and data security obligations on websites and data brokers); California Consumer Privacy Act of 2018, 2018 Cal. Stat. ch. 55 § 3 (AB 375) (limiting collection and sale of consumer data); 2008 740 Ill. Comp. Stat. §§ 14/1-14/99 (barring use of biometric identification without consent).

37. *See, e.g.*, DATA BROKERS, *supra* note 24, at 22, 29; *see generally* FRANK PASQUALE, THE BLACK BOX SOCIETY (2016), especially ch. 2, 5; *Offer You Cannot Refuse, supra* note 24, *passim* (discussing prevalence of various forms of surveillance of online activity).

38. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy,* 114 COLUM. L. REV. 583, 590-606 (2014) [hereinafter *New Common Law of Privacy*].

39. *E.g.*, FTC, PRIVACY ONLINE: A REPORT TO CONGRESS ii-iii (June 1998), https://perma.cc/C4FZ-UHZP (stating that while more than 85% of websites surveyed collected personal information, only 14% provided any notice at all, and only 2% had a "comprehensive privacy policy"). Similarly, a survey by EPIC found that in 1997, only 17 of the top 100 websites

Online entities responded by including privacy policies on their websites, which then became a hook for FTC enforcement.[40] If an entity did not do what its privacy policy said it would, the agency could pursue claims that it had engaged in "deceptive" practices.[41] Over time, these enforcement efforts have led to an evolving, if somewhat thin, "common law" of privacy obligations of online entities.[42] The FTC also conducted workshops and issued reports about online privacy issues, which provided ongoing opportunities to admonish industry to respect and protect consumer privacy, at the risk of poisoning the well of online commerce.[43]

The FTC has also issued specific guidance regarding targeted ads, also referred to as online behavioral ads.[44] For particularly sensitive information, the FTC calls for "opt-in" consent, i.e., sensitive information is not to be collected or used unless the individual affirmatively indicates consent. For non-sensitive information—such as browsing history, clickstreams, and general location information—the FTC calls for "opt-out" consent, which means that the individual is deemed to have agreed to the collection and use of the information unless she affirmatively indicates that she does not want it to happen.[45]

E. The Economics of Privacy under Notice-and-Choice

A key premise of the notice-and-choice model is that individuals have some control over what information is collected about them and how it is used. Those

---

had privacy policies. *See Offer You Cannot Refuse*, *supra* note 24, at 279.

40. Also, in 2003, California enacted a statute requiring any website or online service that collected data about California residents to include a privacy policy that met certain requirements. CALIF. BUS. & PROFS. CODE §§ 22575-579. Any website operated by any United States company could be accessed by Californians, so the law effectively required all domestic online entities to post privacy policies.

41. 15 U.S.C. § 45.

42. *New Common Law of Privacy, supra* note 38 *passim*.

43. *See infra* Part III.C. A full listing of the FTC's reports, workshops, etc. addressing online privacy issues is provided in FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE app. A (2012) [hereinafter FTC, PROTECTING CONSUMER PRIVACY], https://perma.cc/6DCW-FE3C.

44. SELF-REGULATORY PRINCIPLES, *supra* note 25, at 47.

45. *Id.* While the FTC has focused on requiring online entities to follow their privacy policies, it has taken some steps towards enforcing substantive data protection requirements by bringing enforcement actions for having substantively inadequate data protection practices (that is, for "unfair" actions). *See* Fed. Trade Comm'n v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015). *See also Potential FTC Data Protection, supra* note 34. There are limits to how far the FTC can go, however. In LabMD, Inc. v. Fed. Trade Commission, 891 F.3d 1286 (11th Cir. 2018), the court struck down, as unenforceably vague, an FTC "cease and desist" order that effectively required LabMD to "cease" having an unreasonably lax security program.

who collect information say what data will be collected and what will be done with it, and the individual can either grant or withhold consent to (at least some of) that collection and use—if nothing else, by choosing to visit or avoid particular websites or online services.

This model is readily amenable to economic analysis. An individual's right to control the collection or use of information can be viewed as a species of property that can be bought, sold, licensed, etc.[46] As with any property, one can then imagine a market for it. People who sign up for Facebook, for example, buy the right to interact with friends online, while the price they pay (or, equivalently, what they are selling) is permission to surveil their online activities and use the information to serve personally-tailored ads.[47] Similarly, people who use Google for search or email buy access to those functions; as with Facebook, they pay not with money but with permission to surveil them, store and analyze the data, and serve them targeted ads.[48] In either case, the equilibrium "price" observed in the market supposedly reflects an optimal balancing of the interests of buyers and sellers regarding the collection and use of information, and, in the aggregate, an efficient allocation of society's resources.[49]

Both this overall model and the specifics of the economic analysis, however, suffer from a critical flaw: they are largely unrelated to reality. A key concern is that people's assent to be surveilled, to have their data aggregated and analyzed, and to receive targeted ads may not be meaningful. In support of this view, scholars have emphasized the limitations on people's ability to make decisions about complex, contingent, risk-laden, and uncertain future costs.[50] Notably, some of these limitations arise from "problems of self-control and limited self-insight, in which case

46. *E.g.*, Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1196, 1199 (2016) [hereinafter *Information Fiduciaries*].

47. *See generally Unpacking Privacy's Price*, *supra* note 26.

48. Note that neither Google nor Facebook shares the profiles of their users with third party advertisers. Instead, the advertisers specify target demographics, and Google and Facebook then serve the ads to people whose profiles match the advertisers' target groups. The targeting can be remarkably narrow. *See, e.g.*, Brian Swichkow, *The Ultimate Retaliation: How I Pranked My Roommate with Targeted Facebook Ads*, GHOSTINFLUENCE (Sept. 6, 2014), https://perma.cc/G46A-FUD2.

49. Alessandro Acquisti et al., *The Economics of Privacy*, 52 J. ECON. LIT. 442, 448 (2016) ("With a query on a search engine, the searcher is implicitly selling information about her current interests in exchange for finding relevant results. By using an online social network, members are implicitly selling information about their interests, demographics, and networks of friends and acquaintances, in exchange for a new method of interacting with them. Applying the principle of revealed preference, we could infer people's valuations for their personal data by observing their usage of those tools.").

50. Alessandro Acquisti, *From the Economics to the Behavioral Economics of Privacy: A Note*,

knowledge 'is insufficient to motivate behavior change.'"[51] In practice, (a) few people read privacy disclosures purportedly explaining what information is collected, what happens to it, and what choices they have; (b) those who try to read them cannot understand them; and (c) even when carefully parsed, many privacy policies are written in a way that obscures what actually happens with the information gathered.[52] As a result, people may understand in general terms that what they are buying is access to a website or social media service, but they have no real idea what it is that they are selling.[53] Even if someone reads a policy and does not like its content, she will be unable to engage in any meaningful bargaining about it—privacy policies are presented on a "take-it-or-leave-it" basis.[54] The practical irrelevance of

---

ETHICS AND POLICY OF BIOMETRICS: THIRD INTERNATIONAL CONFERENCE ON ETHICS AND POLICY OF BIOMETRICS AND INTERNATIONAL DATA SHARING 23 (David Zhang & Ajay Kumar eds., 2010) [hereinafter *From Economics to Behavioral Economics*] ("A growing body of evidence from behavioral and experimental economics has demonstrated that human beings are prone to systematic decision making biases and judgment errors in scenarios involving uncertainty and risk."); Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, 3 IEEE SECURITY & PRIVACY 26, 26-28 (2005) [hereinafter *Privacy and Rationality*]; *Potential FTC Data Protection*, *supra* note 34, at 2282 (noting the "human tendency to make irrational decisions").

51. *From Economics to Behavioral Economics*, *supra* note 50, at 23. While behavioral economics is certainly part of mainstream economic thinking—at least two of its leading thinkers, Daniel Kahneman and Richard Thaler, have received Nobel prizes—some still question its value in formulating legal rules. *E.g.*, Joshua D. Wright & Douglas H. Ginsburg, *Behavioral Law and Economics: Its Origins, Fatal Flaws, and Implications for Liberty*, 106 NW. U. L. REV. 1033, 1053-67 (2012) [hereinafter *Behavioral Law and Economics*].

52. *Information Fiduciaries*, *supra* note 46, at 1199-1200, 1222-24; Sophie C. Boerman et al., *Online Behavioral Advertising: A Literature Review and Research Agenda*, 46 J. ADVERTISING 363, 367-68 (2017) [hereinafter *Behavioral Advertising Literature Review*]; Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 641 (2014) [hereinafter *The Internet's Most Popular Price*]; Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1882-93 (2013) [hereinafter *Privacy Self-Management*].

53. *Privacy and Rationality*, *supra* note 50, at 25 ("The individual decision process with respect to privacy is affected and hampered by multiple factors. Among those, incomplete information, bounded rationality, and systematic psychological deviations from rationality suggest that the assumption of perfect rationality might not adequately capture the nuances of an individual's privacy-sensitive behavior."). *See also From Economics to Behavioral Economics*, *supra* note 50, at 24; *Unpacking Privacy's Price*, *supra* note 26 *passim.* Problems of this nature do not necessarily mean that standard economic analysis cannot be applied to understand what is happening in a market. *See, e.g.*, *Behavioral Law and Economics*, *supra* note 51, at 1052-67. However, the difficulties with using a market model to describe consumer actions surrounding which information online entities collect and what they do with it seem particularly severe.

54. Scott Bender, *Privacy in the Cloud Frontier: Abandoning the "Take it or Leave it" Approach*, 4 DREXEL L. REV. 487, 509-14 (2012) (discussing "take it or leave it" as the norm for online terms of service, including privacy policies). An effort to provide consumers with greater ability to manage their relationships with online entities, including questions of information and privacy, is the "customer commons" championed by *Linux Journal* editor and internet visionary Doc Searls. *See* Doc Searls, *Uber's Pending Sale of Your Personal Data*, DOC SEARLS WEBLOG (Nov. 20, 2016), https://perma.cc/XVY9-Y2FT. A related effort, also supported by Searls, is Project VRM, which stands for "vendor relationship management." *See* PROJECT VRM, https://perma.cc/EC9F-58SX

individual efforts to protect privacy through choices in a market is confirmed by a reluctance of courts to find that privacy violations amount to cognizable harm for purposes of imposing any meaningful monetary or other liability, at least in the absence of a specific statute creating a specific enforceable right to bar the disclosure of specific information.[55] So, people probably do not know what they are buying, they surely do not know what they are selling, and in any case they cannot do anything about it if the bargains they have supposedly struck are violated.[56]

These considerations shed some light on the "paradox of privacy": people say they are concerned about their privacy yet repeatedly take actions that fail to protect it.[57] Although people do, in some sense, acquiesce to being surveilled and bombarded with ads, the limits on human decisionmaking capacity and on people's knowledge of what happens with the data being collected suggest that their consent is much less than fully rational and informed.[58]

More fundamentally, these critiques of a supposed privacy "market" assume a framework in which privacy is a commodity that people bargain away, bit by bit, in exchange for free access to websites, email, etc. Some have challenged that framework, asserting that "privacy" describes a range of shifting, context-dependent social and cultural expectations, not a commodity to be bought and sold.[59] Within this framework, for example, Richards and Hartzog suggest that expectations surrounding privacy arise from relationships of trust.[60] When people trust someone, they

(archived Oct. 26, 2018) ("VRM tools provide customers—that's all of us—with ways to operate with full agency in the marketplace. This includes the ability to control and permit the use of personal data, to assert intentions in ways that can be understood and respected, and to protect personal privacy."); *see also* Michal S. Gal & Niva Elkin-Koren, *Algorithmic Consumers*, 30 HARV. J. LAW & TECH. 309, 312-22 (2017) (discussing how consumers might use algorithms to make purchase decisions). *But see Offer You Cannot Refuse*, *supra* note 24, at 291-93 (discussing technologies used to defeat consumer privacy choices).

55. Neil M. Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. J. 431, 441-44 (2016) [hereinafter *Taking Trust Seriously*] (discussing problems with adjudicating claims of privacy "harm"); *see also* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 738-42 (2018) [hereinafter *Risk and Anxiety*]; *Potential FTC Data Protection*, *supra* note 34, at 2277-80 (discussing courts' reluctance to impose liability for privacy harms).

56. The fact that the legal system cannot provide meaningful redress or compensation for most privacy-based harms has long been noted. *E.g.*, Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L. J. 421, 456-71 (1980).

57. *Taking Trust Seriously*, *supra* note 55, at 446.

58. *From Economics to Behavioral Economics*, *supra* note 50, at 23-24; *Privacy and Rationality*, *supra* note 50, at 25; *Unpacking Privacy's Price*, *supra* note 26 *passim*.

59. *E.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT (2010), ch. 7-9.

60. *Taking Trust Seriously*, *supra* note 55, at 447-51.

expect her not to use what she learns against their interests.[61] Similarly, Balkin argues that online entities can reasonably be viewed as "information fiduciaries," with special obligations not to use consumers' information against them.[62]

One reason for the disconnect between the reality and the rhetoric of the standard model is that the model ignores the social aspects of privacy. To begin to address this failure, some argue that privacy should be viewed as a "public good."[63] A public good is a commodity that is both non-rivalrous and non-exclusive; one person's consumption of it does not prevent another person from enjoying it (non-rivalrous), and once it is produced, everyone will enjoy the benefit of it, even if they do not pay (non-exclusive).[64] A typical example is national defense. Once the military has taken appropriate steps to defend the country, everyone is protected; one individual's protection does not diminish another's; and an individual is protected even if she does not pay her taxes. Privacy, however, does not fit this model particularly well.[65] One can have (at least some) privacy even if others do not, and one can pay for means to enhance and protect privacy that do not benefit others, at least not very much.[66]

A more nuanced view is that each person's decisions about privacy affect others' privacy as well. In economic terms, this means that decisions about privacy have *externalities.*[67] Privacy externalities can arise in several ways. For example, if one person posts a picture of another on Facebook from an event both attended, the second person's privacy has been affected.[68] More subtly, even purely "private" ac-

61. *Id.*

62. *Information Fiduciaries*, *supra* note 46, *passim.*

63. *E.g.*, *Privacy as a Public Good*, *supra* note 28, *passim*; Dennis D. Hirsch, Response, *Privacy, Public Goods, and the Tragedy of the Trust Commons*, 65 DUKE L. J. ONLINE 67, 71-74 (2016); Priscilla M. Regan, Response, *Privacy as a Public Good*, 65 DUKE L. J. ONLINE 51, 52-53, 58-62 (2016); Priscilla M. Regan, *Reviving the Public Trustee Concept and Applying It to Information Privacy Policy*, 76 MD. L. REV. 1025, 1027-28 (2017); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2084-90 (2004). Consistent with the analysis presented here, Professor Hirsch recognizes that online trust (and information about consumers) is best viewed as a common-pool resource used by online entities and is thus subject to a potential "tragedy of the commons." *See* Hirsch, *supra* note 63 at 82-87; *see also infra* note 131.

64. Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, 100 AM. ECON. REV. 641, 642 (2010) [hereinafter *Beyond Markets and States*].

65. *See* Hirsch, *supra* note 63, *passim*; *see also* Froomkin, *supra* note 34, at 1717.

66. For example, one can deploy ad-blocking software. *See infra* Part IV.B.1.

67. *Privacy as a Public Good*, *supra* note 28, at 398, 433.

68. Illinois law bars the use of biometric identification (e.g., identifying someone from a photograph) without consent. *See* 2008 740 Ill. Comp. Stat. §§ 14/1 to 14/99. This has raised ques-

tivity online affects others through the impacts of data mining and predictive marketing. For example, information about which websites someone looks at or what she buys is used to enhance her profile, but that knowledge does not just affect the ads they serve to *her.* The more online entities know about what one person will look at and buy (and at which prices, and in which contexts), the more they also know about how people like her will act.[69] Each contribution to the online profilers' pool of information thus affects everyone.[70]

Still another way to reflect the social aspects of privacy is to view individuals' decisions about whether to share information as an example of a "prisoner's dilemma."[71] In this formulation, privacy is something everyone would like more of, so everyone would be better off if people agreed to "cooperate" by not sharing. At innumerable points of decision, however, people instead "defect" by sharing information.[72] In the classic prisoner's dilemma, defection leads to a longer prison sentence for each criminal than either would face if she cooperated. In the privacy prisoner's dilemma, defection—sharing information—leads not only to online entities having profiles of the individuals choosing to defect, but also to an enhanced ability to induce others (similar to those already profiled) to buy things they would otherwise not buy, at higher prices than they would otherwise pay. From this perspective, enhancing consumer privacy is a collective action problem: how can consumers be motivated to make privacy-enhancing choices even though their short-run interest is always to give up information?[73]

---

tions regarding, for example, the normal operation of automatic photo-tagging capabilities included in services offered by firms such as Shutterfly. *See, e.g.*, *Monroy v. Shutterfly*, 2017 U.S. Dist. LEXIS 149604 (N.D. Ill. Sept. 15, 2017) (denying motion to dismiss purported class action).

69. *Privacy as a Public Good*, *supra* note 28, at 389.

70. Aggregation of information is a distinct type of privacy "harm" to which an individual may be subject. *Privacy Self-Management*, *supra* note 52, at 1881 ("[M]any privacy harms are the result of an aggregation of pieces of data over a period of time by different entities. It is virtually impossible for people to weigh the costs and benefits of revealing information or permitting its use or transfer without an understanding of the potential downstream uses.").

71. *Privacy as a Public Good*, *supra* note 28, at 388-89.

72. *Id.* at 388-89, 391-93, 396-406.

73. *Id.* at 418-21. Cybersecurity expert Bruce Schneier has suggested that online entities also face a "prisoner's dilemma," in which they do not work together as well as they should—and may want to—in order to effectively protect consumer privacy. *See* Bruce Schneier, *Data Privacy as a Prisoner's Dilemma*, SCHNEIER ON SECURITY (July 28, 2011), https://perma.cc/8GH7-WNWV (contending that online entities can and do cooperate in the realm of online privacy but that their underlying objective is to encourage trust rather than to protect privacy).

F. Rejecting the Commodifaction of Privacy

These approaches suffer from a deeper conceptual flaw. The privacy-as-commodity model fails because information about an interaction between two parties—an individual and an online service—does not come from just one of them. It is information about activity that occurred *between* them, and comes from—and in some sense belongs to—both. Why should the fact that someone reads a blog post about some sensitive topic, or the fact that she purchased a certain book, be deemed to belong to the individual, as opposed to the blogger or the bookseller?[74] At least with regard to privacy surrounding browsing, online purchases, and social media, it is not at all obvious that the information should be viewed as the individual's to protect.

This conundrum parallels the question of the assignment of liability in cases where the proximity of two activities generates costs, addressed by the famous Coase Theorem.[75] Coase showed that under certain assumptions, the same economically efficient result will be reached irrespective of how liability is originally assigned.[76] This suggests that if the right to control the use of online information were clearly assigned either to consumers or to online entities, they would reach the efficient solution regarding data use and protection, whatever that solution might be.[77] From this perspective, the key problem is ambiguity about who has the right to control the information. Removing this ambiguity, however, likely would not work in the online economic ecosystem. Coase's result only applies if the parties can negotiate an agreement with negligible transaction costs.[78] Bargaining over in-

74. This problem has been evident since some of the earliest writings on the economics of privacy. *See, e.g.*, Gorge J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 626 (1980) (referring to the "inherent partnership in producing information"); *see also* Richard A. Posner, *An Economic Theory of Privacy*, REGULATION (1978) 19, 21.

75. R.H. Coase, *The Problem of Social Cost*, 3 J. L. & ECON. 1 (1960).

76. One of his examples is fires caused in a wheat field by sparks from trains running on tracks through the field. The fires can be avoided either by installing spark arrestors on the trains (which increases the railroad's costs), or by not planting so close to the tracks (which lowers the farmer's revenue). Suppose that it is more efficient to add spark arrestors. If the railroad is deemed to have the right to decide, the wheat farmer will be motivated to offer to pay the cost of the arrestors to avoid further damage to his fields. If the farmer is deemed to have the right to decide, the farmer will require the railroad to install the arrestors. Either way, the most efficient solution is reached. *Id.* at 31-34.

77. Richard Posner argued that the law does this already. His example was the rule that magazines do not need to get permission from subscribers to sell subscriber lists to third parties. Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 395 (1978).

78. Coase, *supra* note 75, at 15-19.

dividual pieces of information, or even all the information around any one individual, does not scale—the transaction costs would overwhelm the value of the information.[79] Moreover, this approach suffers from the same problems noted above regarding individuals' ability to understand and evaluate the actual costs and risks associated with revealing information about themselves.[80]

While Coasian bargaining is unworkable in the context of online privacy, there is still value in shifting perspective from viewing information as a commodity to seeing it as something that arises in a relationship. The question is how to translate intuitions about privacy expectations developed in more traditional real-life situations into the online context. One idea is to characterize these interactions as creating relationships of trust.[81] From this perspective, Richards and Hartzog characterize the duties of a trustworthy party as honesty, discretion, protection, and loyalty.[82] A similar approach is Balkin's suggestion that online entities become "information fiduciaries," with special duties to protect people whose information they handle.[83] In either case, the asserted duties of online entities are not seen to arise from bargaining. Instead, they are viewed as essentially cultural, inherent in the relationship between an individual and an online service provider.[84] But while it seems clear that society would *want* websites, social media services, etc. to act in this trustworthy manner, it seems equally clear that, in disturbingly many cases, they do not. The reason is obvious: those entities are not in the business of taking care of their users. Instead, they are in the business of making money, and they make money—either as a business model or as a sideline—by collecting, analyzing, aggregating, and selling information about their users.[85] So, while it would be nice if these entities were trustworthy, and they want everyone to think that they are, they

79. *See supra* note 54. One of the goals of the Customer Commons and Project VRM activities referred to in note 54, *supra,* is to find ways to automate this bargaining using browser code indicating what information may be collected on what terms. In economic terms, this is an effort to reduce transaction costs to a sufficiently low level such that an actually bargained-for result could be reached.

80. *See supra* notes 49-53.

81. *Taking Trust Seriously*, *supra* note 55, at 447-51.

82. *Id.* at 459-71.

83. *Information Fiduciaries*, *supra* note 46 *passim.*

84. *See id.*; *see also Behavioral Advertising Literature Review*, supra note 52, at 367-68.

85. A standard formulation of this situation is "if you're not paying, you're the product." *See, e.g.*, Scott Goodson, *If You're Not Paying For It, You Become the Product*, FORBES (Mar. 5, 2012), https://perma.cc/2RHV-JAT3. The idea is not new; it was applied decades ago to broadcast television which, from the broadcaster's perspective, is a business in which consumer eyeballs—the product—are delivered to the real, paying customers, that is, to advertisers. *See* R. Serra & C. Wyergraf, RICHARD SERRA: INTERVIEWS, ETC., 1970-1980 104 (1980).

are not, in fact, particularly trustworthy as that term is defined by Richards and Hartzog.[86]

Even so, it is helpful to reject the notion of information and privacy as market commodities, and instead frame the issue as one of trust. The more people trust that information they give up online will not be abused, the more people are willing to go online even though doing so inevitably reveals information. On the other hand, if people are untrusting and suspicious, they will spend less time and money online. The overall level of trust, therefore, is very important to the online ecosystem, and online entities thus would buy more trust if they could. But it is hard to envision a market for the direct purchase and sale of trust—a subjective emotional state. While trust matters immensely to market transactions, therefore, the economic framework that best captures the way consumers, online entities, and policymakers deal with trust and privacy is not a market. Instead, as described below, it is a commons.

III. THE AMBIENT TRUST COMMONS [87]

The motivations and actions of firms trying to manage a commons differ from those of firms competing in a market. As a result, looking at legal and policy issues surrounding online privacy and trust from within the framework of a commons can illuminate how online firms, consumers, and government entities behave and interact.[88]

A. The Idea of a Commons as an Economic Institution

Economists study how to efficiently allocate scarce resources. Resource allocation occurs within social, political, and economic institutions—markets, governments, firms, etc. Economists have thus studied why and how different institutional arrangements arise to perform the resource allocation function.[89] The traditional

86. For an accessible introduction to the economics of untrustworthiness, *see generally* GEORGE A. AKERLOF & ROBERT J. SHILLER, PHISHING FOR PHOOLS: THE ECONOMICS OF MANIPULATION AND DECEPTION (2015); *see also* ARTHUR A. LEFF, SWINDLING AND SELLING: THE STORY OF LEGAL AND ILLEGAL CONGAMES (1976).

87. The notion of "ambient trust" derives from the concept of "ambient connectivity" championed in the broadband policy area by Bob Frankston (co-inventor of VisiCalc). Bob Frankston, *Ambient Connectivity: An Introduction*, WRITINGS AND MUSINGS (Sep. 27, 2009), https://perma.cc/TT7D-N2NB (discussion of ambient connectivity).

88. *See supra* note 8 and accompanying text.

89. *E.g.*, ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (1990) [hereinafter GOVERNING THE COMMONS]; OLIVER WILLIAMSON, MARKETS AND HIERARCHIES (1975); *see also* JACK KNIGHT & ITAI SENED, EDS., EXPLAINING SOCIAL

view has been that competitive markets are the best way to efficiently allocate resources. Competition among sellers drives price down to marginal cost,[90] which means consumers benefit—in the form of maximum "consumer surplus"—from the lowest achievable price for what they buy.[91] When these conditions are present across all markets, consumers benefit from an efficient allocation of resources among all goods and services, given the relative costs of producing them and the distribution of consumer demand for them. Ubiquitous competitive markets get people as much of what they want as our economy and technology can deliver, at prices that reflect the relative costs of the resources used to produce them.[92]

While markets do this in the abstract, the reality is more complicated. For example, nearly a century ago, economists noted a conundrum: if markets are so efficient, why are there firms? A firm allocates resources within its domain through a command-and-control system, not by relying on supply and demand. If markets were really the most efficient way to allocate resources, there would be no reason for these fiefdoms of command-and-control allocation. One answer was provided by Coase, who recognized that there are costs to engaging in market transactions (notably the cost of learning what goods and services are available at what prices, and the cost of negotiating contracts), and that it can be cheaper to avoid those costs by establishing a command-and-control organization to allocate resources within it.[93] Organizations that are too small incur costs from engaging in market transactions that larger firms avoid. On the other hand, a large organization incurs costs

---

INSTITUTIONS (1998).

90. Marginal cost is the cost the seller incurs in making one more unit of the item being sold. As long as the seller receives at least that much in payment for that unit, she will be willing to produce and sell it.

91. Consumer surplus is the difference between what a consumer would be willing to pay for something and what she pays. The lower the price, the greater the consumer surplus. J.R. Hicks, *The Rehabilitation of Consumers' Surplus,* 8 REV. ECON. STUD. 108, 108 (1941); *see also* Economic Surplus, WIKIPEDIA, https://perma.cc/Z3QX-7CZX (archived Nov. 14, 2018).

92. In that case, output would be on the "production possibility frontier," which means all available production efficiencies have been realized, the only way to produce more of any one thing is to produce less of something else, and the only way to make one person better off (by getting them more stuff) is to make someone else worse off (by getting them less). This is called "Pareto optimality." Note that the *distribution* of wealth and income is a different question. A situation where one individual controls 99% of wealth is just as Pareto-optimal as one where everyone has an equal share. The agnosticism of Pareto optimality regarding issues of distribution can obscure important conflicts—ultimately political, not economic, in nature—among different groups within the economy. *Cf.* Robert MacColloch, *Income Inequality and the Taste for Revolution,* 48 J. LAW & ECON. 93, 94, 103-114 (2005) (survey-based analysis showing that increases in income inequality lead to increased support for revolution).

93. R.H. Coase, *The Nature of the Firm,* 4 (16) ECONOMICA 386, 390-98 (1937).

coordinating internal resource allocation that smaller firms avoid. As markets become more efficient (for example, due to improved access to information), those internal costs can no longer be justified, and the optimal firm size declines. On the other hand, as command-and-control decision-making becomes more efficient (for example, due to improved techniques for analyzing internal operations), the optimal firm size grows. This helps explain why economic institutions are not limited to markets.[94]

Analyzing institutions in terms of the relative transaction costs incurred in markets versus hierarchies explains why competitors are often firms rather than individuals, but it does not explain why firms—which compete both as sellers (for the business of their customers) and as buyers (for inputs they need)—also sometimes cooperate. How and why do competitors choose to cooperate? Sometimes cooperation is simply an effort to obtain extra profits at the expense of consumers, such as an agreement to divide markets or fix prices.[95] But sometimes cooperation enhances consumer welfare rather than degrading it. Recognizing this, antitrust law—America's "comprehensive charter of economic liberty"[96]—tolerates competitors working together in many contexts, from trade associations[97] to standard-setting bodies[98] to joint ventures.[99] These kinds of activities are evaluated using the "rule of reason," which considers whether, on balance, the cooperation helps or hurts consumers.[100]

A commons is a distinctive form of cooperative institution that arises when competing producers share access to a resource that grows or replenishes itself at some rate, and thus can be used by the producers, but that is subject to catastrophic decline (called "collapse") if it is overused/over-harvested.[101] The classic examples of commons are herders sharing a field on which to graze their animals, or fishermen sharing a fishery.[102] Collapse occurs when the users remove so much of the

94. *See also* WILLIAMSON, *supra* note 89, at ix, xi.

95. As Adam Smith observed, "People of the same trade seldom meet together, even for merriment and diversion, but the conversation ends in a conspiracy against the public, or in some contrivance to raise prices." ADAM SMITH, THE WEALTH OF NATIONS Book I, ch. X (1776).

96. Northern Pac. R.R. Co. v. United States, 356 U.S. 1, 4 (1958).

97. Nat'l Soc'y of Prof. Eng. v. United States, 435 U.S. 679 (1978).

98. Allied Tube & Conduit Corp. v. Indian Head, Inc., 486 U.S. 492 (1988); Am. Soc'y. of Mechanical Eng. v. Hydrolevel Corp., 456 U.S. 556 (1982).

99. Texaco Inc. v. Dagher, 547 U.S. 1 (2006).

100. Continental TV v. GTE Sylvania, Inc., 433 U.S. 36, 49-59 (1977) (describing rule of reason).

101. GOVERNING THE COMMONS, *supra* note 89, at 2-3, 15-21, 30-31.

102. *See, e.g.*, Hirsch, *supra* note 63 *passim.*

common-pool resource that it cannot replenish itself and its supply sharply declines (perhaps to zero).[103] If the users manage it well, however, it can be exploited by all of them over an extended period of time.

Even where a resource is shared and collapse is possible, sometimes the best way to avoid it is to eliminate the "commons" aspect—the shared use—and instead establish a system of unambiguous property rights, so each entity owns a piece of the resource and will want to use it efficiently.[104] But there are situations in which a resource is used in common and is subject to collapse if overused, but cannot readily be converted to excludable property rights. In such cases, in order to avoid a collapse, the producers will have a strong incentive to organize into a commons and establish rules to fairly allocate the resource while ensuring that the overall level of resource use is sustainable.

For some time, the dominant notion of a commons was that it was something that inevitably and tragically failed.[105] The danger of collapse can be particularly troubling where the common-pool resource has a non-linear response to more intense harvesting. In such cases, small increases in the use of the resource initially produce small declines in its level, but at some point an additional small increase yields a rapid and perhaps irreversible decline.[106] Notwithstanding this danger, however, in the real world commons are often made to work.[107] In analyzing a commons, the focus is on avoiding collapse by means of fair and workable rules for managing the resource and imposing a governance structure that credibly enforces the rules against cheating by individual members.[108]

It bears emphasis that in the United States economy, commons aren't that common. Markets, private hierarchies (firms), and/or public ones (governments) are the

---

103. Garrett Hardin, *The Tragedy of the Commons,* 162 SCIENCE 1243, 1244 (1968), https://perma.cc/HCP5-SH2F.

104. For example, Coase suggested that the FCC adopt this approach for allocating the rights to use spectrum. *See* R.H. Coase, *The Federal Communications Commission,* 2 J. LAW & ECON. 1, 14, 17, 25-35 (1959). More broadly, Polanyi recounts the decades-long process of converting "common" property in England to enclosed, private fields. *See generally* KARL POLANYI, THE GREAT TRANSFORMATION (1945).

105. Hardin, *supra* note 103, *passim;* GOVERNING THE COMMONS, *supra* note 89, at 2-3, 7.

106. *See, e.g.*, Marten Scheffer et al., *Catastrophic Shifts in Ecosystems,* 413 NATURE 591 (2001). Collapse of a resource under stress is analogous to non-linear "phase transitions" that occur in various physical and abstract systems, such as water turning to ice or the portion of formerly isolated network nodes that become directly or indirectly connected as more and more point-to-point connections are added. *See* STUART KAUFFMAN, AT HOME IN THE UNIVERSE (1995), especially ch. 3, "We the Expected."

107. GOVERNING THE COMMONS, *supra* note 89 *passim.*

108. *Id. See also Beyond Markets and States, supra* note 64, at 653.

norm. This is so for several reasons. First, for most of the economy there is a functioning regime of private property rights that permits markets to work. Second, even when markets have flaws, the most effective response is often regulation or taxation to address them. Third, even where a commons might address resource allocation issues, it may be more effective to impose property rights via regulation.[109] Fourth, United States antitrust laws create significant potential liability when firms cooperate. This is particularly true for activities that smack of market division and price fixing, which are *per se* illegal. While careful allocation of access to an exhaustible resource is at the heart of managing a commons, at first blush such arrangements can look like an agreement not to compete in exploiting the resource. United States antitrust law, therefore, likely suppresses the development and establishment of commons even in situations where they might be beneficial.[110] For all these reasons, then, it should not be surprising that—despite their intellectual interest—finding commons in the wild, so to speak, is uncommon.[111]

109. *E.g.*, Hirsch, *supra* note 63; *see also* Carol M. Rose, *Rethinking Environmental Controls: Management Strategies for Common Resources,* 1991 DUKE L. J. 1, 31-38 (1991) [hereinafter *Rethinking Environmental Controls*] at 9-10, 21-24 (discussing creating property rights as a way to manage a common-pool resource). From this perspective, intellectual property law—protection of inventions and writings by government fiat—amounts to taking what might otherwise be "common" resources—knowledge and ideas—and creating artificial property rights in them to encourage their management. *See generally* RONALD V. BETTIG, COPYRIGHTING CULTURE: THE POLITICAL ECONOMY OF INTELLECTUAL PROPERTY (1996) *passim*; JAMES BOYLE, THE PUBLIC DOMAIN: ENCLOSING THE COMMONS OF THE MIND (2008), especially ch. 1-3 & 7; LEWIS HYDE, COMMON AS AIR (2010), especially ch. 3. But the "commons" aspect of intellectual property can still be seen, for example, in rules requiring the "fair, reasonable and non-discriminatory" licensing of patents essential to complying with an industry standard. *See, e.g.,* Apple v. Motorola, 869 F. Supp. 2d 901 (2012), *aff'd*, 757 F. 3d 1286 (Fed. Cir. 2014). More broadly, the transformation of agriculture and herding in England from a commons-based system to privately managed property—the process of "enclosure"—disrupted centuries-old practices, but also increased the productivity of the newly enclosed land. *See* POLANYI, *supra* note 104.

110. Jonathan H. Adler, *Conservation Through Collusion: Antitrust as an Obstacle to Marine Resource Conservation,* 61 WASH. & LEE L. REV. 3, 24 (2004) ("What conservation demands, antitrust condemns"); *see also id.* at 20-38. One can find commons-like arrangements where the antitrust laws do not apply, such as lobbying—an activity immune from antitrust liability under *Eastern Railroads Presidents Conference v. Noerr Motor Freight, Inc.*, 365 U.S. 127 (1961) and *United Mine Workers v. Pennington*, 381 U.S. 657, 660 (1965). The members of a lobbying group are seeking to manage and maintain a favorable legislative or regulatory environment—surely a common resource. All members of an industry are typically subject to the same laws and all can be harmed by a catastrophic decline in the benign nature of those laws, so motivations similar to those engendering the creation of natural resource commons apply to lobbying groups.

111. There are a reasonable number of federal court references to Hardin's "tragedy of the commons," but electronic research reveals not a single court case citing Ostrom's more positive analysis of how and why commons work. This may reflect the power of the "tragedy" metaphor, or it may just be that tragic situations are more likely to lead to litigation.

Creating a functioning commons—even when the underlying conditions would make one useful—can be hard. As Ostrom notes,

> All efforts to organize collective action, whether by an external ruler, an entrepreneur, or a set of principals who wish to gain collective benefits, must address a common set of problems. These have to do with coping with free-riding, solving commitment problems, arranging for the supply of new institutions, and monitoring individual compliance with sets of rules.[112]

Ostrom identified eight organizational tasks needed to develop a sustainable commons:

1. Define clear group boundaries.
2. Match rules governing use of common goods to local needs and conditions.
3. Ensure that those affected by the rules can participate in modifying the rules
4. Make sure the rule-making rights of community members are respected by outside authorities.
5. Develop a system, carried out by community members, for monitoring members' behavior.
6. Use graduated sanctions for rule violators.
7. Provide accessible, low-cost means for dispute resolution.
8. Build responsibility for governing the common resource in nested tiers from the lowest level up to the entire interconnected system.[113]

The discussion below explains why it makes sense to view the stock of online ambient trust as a common-pool resource, and how the commons managers—firms in the online economic ecosystem—have risen to the challenge of making the ambient trust commons work to avoid collapse.

112. GOVERNING THE COMMONS, *supra* note 89, at 27.

113. GOVERNING THE COMMONS, *supra* note 89, at 90, 88-102; *Beyond Markets and States, supra* note 64, at 653.

B. The Idea of Ambient Trust

A great deal of literature addresses what trust is, what causes it to arise, and how it affects social and economic relationships.[114] A reasonable shorthand is that trust is a belief that one person will act in another's interest (help them, or at least leave them alone) when the person has the opportunity, and perhaps the incentive, to do harm. Thus, we speak of trusting someone "with" power or resources or information, but tend not to worry about someone (such as a small child) who has no ability to do harm, *i.e.,* no power. That lack of concern, however, doesn't mean that the powerless person is "trusted" in any meaningful sense. Conversely, trust is destroyed when one person exploits or harms the other—in Richards & Hartzog's terms, when someone violates duties of honesty (lies to us), discretion (blabs our secrets), protection (fails to take care of us), or loyalty (works against us).[115] The nature and amount of trust created by honorable dealings or destroyed by treachery will depend on the expectations of the trusting party going into the relationship, the nature and degree of a betrayal, etc.[116]

At first blush, it may seem that the more trust there is, the better off everyone will be. That might be true if everyone were trustworthy. Unfortunately, that's not the case. As a result, too much trust isn't good or admirable. It's naïve, potentially even stupid. This means that it makes no sense to try (via custom, law, or regulation) to create a world that encourages complete trust, because there will always be bad actors who can and will abuse it.[117]

---

114. *E.g.*, Jin-Hee Cho & Kevin Chan, *A Survey on Trust Modeling,* 48 ACM COMPUTING SURVEYS, No. 2, art. 28 (2015); Frank B. Cross, *Law and Trust,* 93 GEO. L.J. 1457 (2005); Julia Y. Lee, *Trust and Social Commerce,* 77 U. PITT. L. REV. 137 (2015); Levent V. Orman, *Bayesian Inferences in Trust Networks,* 4 ACM TRANSACTIONS ON MANAGEMENT INFORMATION SYSTEMS No. 2, art. 7 (2013); Neal Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review,* 126 YALE L. J. 1181 (2017); *Taking Trust Seriously, supra* note 55, at 448-56; Carol M. Rose, *Trust in the Mirror of Betrayal,* 75 B.U.L. REV. 531 (1995); Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World,* 69 U. MIAMI L. REV. 559 (Spring 2015).

115. *Taking Trust Seriously, supra* note 55, at 459-71.

116. Cross, *supra* note 114, at 1462-63; Hirsch, *supra* note 63, at 85 ("Each trustworthy digital interaction reaffirms and enhances [trust], and each abuse of our personal information erodes it."); Richards & Hartzog, *supra* note 114, at 1215-19; *Taking Trust Seriously, supra* note 55, at 460 ("In information relationships, the quickest way to betray a trust is indiscretion: revealing personal information to the wrong person or in the wrong way."); Waldman, *supra* note 114, at 1462-63.

117. A community of trusting individuals is not stable: they are prey for unscrupulous entities. *See* AKERLOF & SHILLER, *supra* note 86, especially Part 2. In the prisoner's dilemma context, a group of "always cooperate" algorithms—analogous to a trusting community—loses to an "always defect" algorithm. ROBERT AXELROD, THE EVOLUTION OF COOPERATION (revised ed. 2006), ch. 2. But the most successful strategy isn't "always defect"; it's a form of "tit for tat," where the algorithm starts out cooperating, but then cooperates or retaliates, based on what its opposite number

This raises the question of why trust is valuable, as opposed to merely being pleasant. The answer, to use a metaphor, is that trust is a transaction catalyst. In chemistry, a catalyst participates in and facilitates chemical reactions, but is not itself used up in those reactions.[118] Trust plays the same role for economic and social activity—it facilitates transactions and interactions, but is not used up in them. To the contrary, as long as trust is not abused, it will tend to increase.[119] In this way, trust lowers transaction costs by making it unnecessary to worry about (at least some of) the endless forms of treachery to which people are potentially subject.[120] An environment of trust lets people avoid the economic costs of protecting against fraud, deceit, etc. in commercial settings, and the psychic costs of protecting against dishonesty and betrayal in interpersonal settings.[121] So, an environment of ambient trust is not just a happier place to live—though it is that—it's also a place where more social and economic wealth is created.[122]

Trust, then, is an individual, subjective phenomenon, but it also has a cultural and social aspect. A society or culture in which most people and entities are mostly trustworthy will support a general assumption of trustworthiness and encourage feelings of trust—and economic and social interaction—until those feelings are abused. A reasonably high level of ambient trust is good for business, so businesses will want to promote it by letting people know that in general, they are trustworthy—that their ads are truthful, that their products perform as advertised, etc. Groups such as the Better Business Bureau embody efforts to encourage consumers to trust what businesses say in their advertisements, and thus to encourage commerce in general.[123]

---

did in the prior round. A particularly effective version adds a touch of forgiveness, occasionally cooperating even in the face of a defection by the other algorithm. *See* Colm O'Riordan, *A Forgiving Strategy for the Iterated Prisoner's Dilemma,* 3 J. ARTIFICIAL SOCIETIES AND SOCIAL SIMULATION No. 4 (2000), https://perma.cc/XM3V-N5PF.

118. *See* KAUFFMAN, *supra* note 106, especially ch. 3. *See also* Catalysis, WIKIPEDIA, https://perma.cc/3A7A-K8ML (archived Nov. 18, 2018).

119. Hirsch, *supra* note 63, at 84 ("Trust naturally replenishes itself. It is a renewable resource.").

120. Larry E. Ribstein, *Law v. Trust,* 81 B.U.L. REV. 553, 553 (2001) ("Trust is a kind of social glue that allows people to interact at low transaction costs.").

121. Eric Posner, *The Law, Economics, and Psychology of Manipulation* (Coase-Sandor Working Paper Series in Law and Economics No. 726, 2015) at 9.

122. Economists recognize that trust promotes economic growth. *E.g.*, Christian Bjørnskov, *How Does Social Trust Affect Economic Growth?,* 78 SO. ECON. J. 1346, 1346 (2012) ("One of the most important and robust results emerging from the . . . empirical literature is indeed that countries with high levels of social trust . . . have grown faster in recent decades than other comparable countries").

123. The BBB's website states: "Better Business Bureau®—Start with Trust®—An ethical

While in the abstract businesses and governments may want to eliminate all dishonesty and fraud, given human nature, that isn't possible, and efforts at suppression will eventually reach a point of diminishing returns.[124] At some point, the negative consequences of as-yet-unsuppressed treachery are small enough that the costs of further policing efforts are not justified by the benefit of eliminating it. In the economic realm, if one type of conduct is proscribed, firms will learn to engage in behavior that—while still preying on consumers—involves conduct that is sufficiently subtle that the exploitation is hard to detect or that does not clearly fall within the prohibited category.[125] The result is that, as long as there is money to be made taking advantage of consumer vulnerabilities (ignorance, impulsive buying, confusion, bounded rationality, gullibility), some level of deceptive, untrustworthy behavior will continue to exist.

Diminishing returns can arise in a somewhat paradoxical sense as well: The more public and aggressive enforcement efforts become, the more people become aware of the problem of treachery, leading people to assume it is widespread—an assumption that, in itself, degrades trust. In the extreme, a general understanding that treachery is normal will normalize treachery, thus frustrating efforts to limit it.[126] For this reason, widespread publicity about strong enforcement efforts will make sense if some particularly notable act of fraud or deceit has become public—essentially, to emphasize the unusual nature of the fraud—but then die down as people become reassured that the incident was unusual.[127] Ultimately, because it is

---

marketplace where buyers and sellers trust each other;" http://perma.cc/ZVU4-FN8D (archived Dec. 16, 2018); "BBB helps consumers identify trustworthy businesses, and those that aren't, through more than 5 million BBB Business Profiles;" and "BBB coaches businesses on ethical behavior and how to build stronger, more trusting relationships with their customers." *See* https://perma.cc/98LC-JWCQ (archived Dec. 16, 2018).

124. *E.g.*, Gary S. Becker, *Crime and Punishment: An Economic Approach,* 76 J. POL. ECON. 169 (1968); Keith N. Hylton, *Optimal Law Enforcement and Victim Precaution,* 27 RAND J. ECON. 197 (Spring 1996).

125. *Id.*; LEFF, *supra* note 86, at 109-110. As Congress noted in passing the FTC Act, "It is impossible to frame definitions which embrace all unfair practices. There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again." H.R. Rep. No. 63-1142, at 19 (1914) (Conf. Rep.). Note also that firms, lacking emotions such as guilt, are a perfect embodiment of Holmes' "bad man," who cares not at all for the purpose or morality behind the law, but instead only about which behaviors will be punished. Oliver Wendell Holmes, Jr., *The Path of the Law,* 10 HARV. L. REV. 457 (1897), *reprinted as* Oliver Wendell Holmes, Jr., *The Path of the Law,* 110 HARV. L. REV. 991, 992-93 (1997).

126. *See Rethinking Environmental Controls, supra* note 109, at 31 (citing THOMAS SCHELLING, MICROMOTIVES AND MACROBEHAVIOR 131 (1982) for the point that sometimes even "one instance of noncooperation may ruin a whole system" of common resource management).

127. *See Digital Market Manipulation, supra* note 27, at 1043 (noting that the FTC typically

impossible to eliminate all bad behavior, and because at some point it isn't worth trying, there will be an equilibrium level of bad behavior with which consumers have to deal, and against which they need to arm themselves.

While there are a wide range of formal and informal models of trust,[128] the details don't matter here as long as the model reflects the following basic characteristics:

1. People have some baseline level of trust in businesses in general and online entities in particular.
2. Trust increases as people interact with online businesses without becoming aware of betrayals attributable to the businesses they deal with.
3. Trust decreases when people directly experience betrayals or learn about businesses betraying others.

One can imagine many adjustments to this basic model. For example, direct experience of betrayal may matter more than hearing about others being betrayed. Businesses will have different specific reputations with different consumers. Recent experience probably matters more than older experience. Specific reports, from reliable sources, of treachery by specific entities may matter more than random rumors of bad behavior. But these refinements are unnecessary here. The upshot of the basic model—however embellished—is the notion of ambient trust. At any given time, people in general have baseline assumptions, shared by most others, as to the trustworthiness of businesses in general, and online businesses in particular. That baseline is maintained or raised as people interact with businesses and do not learn that they have been betrayed. And it is eroded by an individual's negative experiences with individual businesses and by others' reports of betrayals.[129]

If businesses in general are trustworthy and known to be so, people will be more willing to transact business. In the proverbial small town where everybody

---

brings enforcement actions against either very large entities (whose behavior everyone naturally attends to) or very bad entities (companies of any size whose conduct is sufficiently egregious)). Professor Vladeck suggests that regulators can use "shaming" to deal with companies that go too far in manipulating consumers online—that is, "publicizing companies that cross the line from marketing into outright manipulation. Consumers would likely be outraged to learn that companies are manipulating them by identifying and exploiting their weaknesses." Vladeck, *supra* note 28, at 169. *Cf. Rethinking Environmental Controls, supra* note 109, at 31-38 (1991) (discussing the role of norms in assisting in the management of a common-pool resource).

128. *See, e.g.*, Cho & Chan, *supra* note 114.

129. The relevant betrayals need not even be by online businesses. Professor Hirsch notes that following Edward Snowden's revelation of massive governmental surveillance of consumers' web usage, "Google searches for controversial terms decreased . . . [including] terms such as 'herpes,' 'eating disorder' and 'erectile dysfunction." Hirsch, *supra* note 63, at 83-84 (footnotes omitted).

knows everybody, one can rely on reputation (from the past) to provide a decent guide to whom to trust, and a merchant's fear of loss of reputation (for the future) to keep them reasonably honest on an ongoing basis. On the internet, firms in the online economic ecosystem need people to feel relaxed so that they will continue to engage in the online behaviors that provide information and maximize the viewing of advertisements. Anything that would cause people to feel suspicious, threatened, or abused will discourage them from showing up online and put the consumer internet business model at risk. From the perspective of the online ecosystem, then, the stock of consumer trust is a common-pool resource shared by the entities that collect and use information about consumers.

While online businesses depend on the existence of trust, at the same time, there are many ways they can and do take advantage of it. Within Richards' and Hartzog's framework, they can fail to be honest about what information they are collecting and what they will do with it; they can fail to be discreet, by sharing information with third parties; they can fail to protect information adequately, exposing users to embarrassment or (in the case of identity theft) to financial harm; and, fundamentally, they can fail to be loyal, by using the information against their users. They do this by facilitating the efforts of third parties not merely to show ads for things users might be interested in, but to use the information to induce users to buy things they would not, upon reflection, want to buy, at prices as high as possible. All of those activities, if understood by consumers to be the work of online businesses, would tend to erode ambient trust.[130] But as long as the betrayals are

130. *The Internet's Most Popular Price, supra* note 52, at 632. *See also id.* at 221 ("Once the full context is revealed, those who have been manipulated tend to feel used. They ask: *Why wasn't I allowed to decide for myself?*"); Posner, *supra* note 121, at 1; Cass Sunstein, *Fifty Shades of Manipulation,* 1 J. MARKETING BEHAV. 213, 217 (2016) ("Often the distinguishing mark of manipulation is a justified sense of ex post betrayal"). The process of surveilling consumers to get the information on which targeted ads are based can be problematic, and many such practices—including placing "spyware" on a user's computer, unexpectedly (or surreptitiously) uploading and using information on a user's device (such as contact lists), tracking a user's detailed location, and simply sending targeted ads with individualized prices—erode consumer trust in the online environment. The FTC has highlighted these behaviors in settlements with firms that did not live up to their privacy obligations. *See, e.g.*, FTC Press Release, *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers "Brightest Flashlight" App Shared Users' Location, Device ID Without Consumers' Knowledge* (Dec. 5, 2013), https://perma.cc/2B66-5AB5; FTC Press Release, *FTC Approves Final Settlement With Facebook: Facebook Must Obtain Consumers' Consent Before Sharing Their Information Beyond Established Privacy Settings* (Aug. 10, 2012), https://perma.cc/CU4Q-3ZUY; FTC Press Release, *FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network; Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data* (Mar. 30, 2011), https://perma.cc/SYZ5-ZTTT.

sufficiently minor and subtle—or remain unknown—the level of ambient trust will remain high enough for the online ecosystem to continue to function.

All entities in the online ecosystem, therefore, depend on a reasonably high level of ambient trust. All of them, however, also profit by taking actions which have the potential to undermine or destroy trust. While a particular bad actor undertaking particularly bad acts will be singled out to some degree, significant breaches of trust by any online entity will tend to erode trust in all of them. As a result, the level of ambient trust is a common-pool resource for the online ecosystem. Everyone needs it, but everyone exploits it for profit.[131]

C. Creating and Maintaining the Online Ambient Trust Commons

A key challenge for users of a common-pool resource is to organize themselves around a set of enforceable rules that will limit their exploitation of the resource to levels that do not cause collapse—despite short-term temptations to do so.[132] This process can be facilitated by an outside force, such as the government, which can assist in the process of organization, provide a forum for adjudicating disputes, and sanction those who break the rules.[133] In the case of the online ambient trust commons, that role has been played the by FTC.

Ambient trust has always existed in society, and to some extent businesses have always understood that they benefit when consumers can trust them to act ethically. To that end, consumer protection laws, which are intended to outlaw and punish certain forms of untrustworthy behavior, raise the level of ambient trust by creating an environment where people can safely assume that certain types of exploitation

131. *See* Hirsch, *supra* note 63, at 82-87. Professor Hirsch recognizes that ambient trust is a common-pool resource for members of the online economic ecosystem, and thus potentially subject to a "tragedy of the commons," and, indeed, as of this writing his article appears to be the only example in the literature of viewing things this way. However, he does not consider how those entities have managed to avoid collapse (Part III.C. *infra*), how ambient trust differs from the natural resources that are typically addressed by a commons (Part III.D., *infra*), or the unique nature of the economic conflicts between online entities and the consumers whose trust they use and how to address them (Part IV, *infra*).

132. *Id.* at 125-31 (discussing why resource users "don't . . . want to be saved from themselves"). Shi-Ling Hsu, *What is A Tragedy of the Commons? Overfishing and the Campaign Spending Problem,* 69 ALB. L. REV. 75, 77-78 (2005) (defining a true "tragedy of the commons" as involving situations where the users of the common resource "are detracting from their own ability to continue to exploit the resource"); Barton H. Thompson, Jr., *Tragically Difficult: The Obstacles to Governing the Commons,* 30 ENVTL. L. 241, 255-65 (2000) (discussing multiple challenges to establishing a functioning regime to manage a resource even if all users would benefit from such management).

133. GOVERNING THE COMMONS, *supra* note 89 at 18.

are unlikely to occur. From this perspective, building the online ambient trust commons entailed ensuring that the traditional combination of self-regulation (via industry groups) and government oversight (consumer protection laws) was extended, in some form, to the online environment.

The FTC took on this task. It did so at first by calling on industry to recognize their common interest in maintaining consumer trust and by helping participants in the online ecosystem manage their own (and each other's) use of the common trust resource. For example, in a 1998 report, the agency stated,[134]

> Clearly, consumers care deeply about the privacy and security of their personal information in the online environment and are looking for greater protections. These findings suggest that *consumers will continue to distrust online companies and will remain wary of engaging in electronic commerce until meaningful and effective consumer privacy protections are implemented in the online marketplace. If such protections are not implemented, the online marketplace will fail to reach its full potential.*

In a July 1999 Report, the FTC stated,

> For almost as long as there has been an online marketplace, the Commission has been deeply involved in addressing online privacy issues. The Commission's goal has been to understand this new marketplace and its information practices, to assess the impact of these practices on consumers, *and to encourage and facilitate effective self-regulation as the preferred approach to protecting consumer privacy online.* The Commission's efforts have been based on the belief that greater protection of personal privacy on the Web will not only benefit consumers, *but also benefit industry by increasing consumer confidence and ultimately their participation in the online marketplace*.[135]

Later in the same report, the FTC stated,

134. FTC, PRIVACY ONLINE: A REPORT TO CONGRESS, 3-4 (June 1998) (emphasis added), https://perma.cc/C4FZ-UHZP.

135. FTC, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 3 (July 1999) (emphasis added) (endnote omitted), https://perma.cc/K6JT-F8YD.

> Finally, industry must work together with government and consumer groups to educate consumers about privacy protection on the Internet. *The ultimate goal of such efforts, together with effective self-regulation, will be heightened consumer acceptance and confidence.* Industry should also redouble its efforts to develop effective technology to provide consumers with tools they can use to safeguard their own privacy online.[136]

In its report in 2000 urging online entities to embrace the FIPs in their privacy practices, the FTC noted that consumers were concerned about how online entities would handle their data, and observed that consumers

> fear privacy intrusions on the Internet. *This apprehension likely translates into lost online sales due to lack of confidence in how personal data will be handled.* Indeed, surveys show that *those consumers most concerned about threats to their privacy online are the least likely to engage in online commerce,* and many consumers who have never made an online purchase identify privacy concerns as a key reason for their inaction. One study estimates that privacy concerns may have resulted in as much as $2.8 billion in lost online retail sales in 1999, while another suggests potential losses of up to $18 billion by 2002 (compared to a projected total of $40 billion in online sales), if nothing is done to allay consumer concerns.[137]

As time went on, the FTC continued to remind industry of the importance of maintaining consumer trust, with the risk that failing to do so would depress the online market as a whole.[138] These FTC exhortations amount to, in effect, rallying

136. *Id.* at 13 (emphasis added). Commissioner Anthony dissented from the report's conclusion that legislation was not needed: "I am concerned that *the absence of effective privacy protections will undermine consumer confidence and hinder the advancement of electronic commerce and trade*." *Id.,* Statement of Commissioner Sheila F. Anthony Concurring in Part and Dissenting in Part (emphasis added).

137. FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 2 (May 2000) [hereinafter FAIR INFORMATION PRACTICES], https://perma.cc/CY8H-2SD6.

138. *See* FTC, PROTECTING CONSUMER PRIVACY, *supra* note 43, app. A (providing a complete listing (as of 2012) of FTC reports addressing privacy issues, as well as various staff-level workshops and other agency activities addressing these issues).

the potential managers of the online trust commons to recognize their mutual interests in promoting the growth of, and avoiding over-use of, the common-pool trust resource. Here is a final example from the agency's most recent (2012) report dealing with online consumer privacy:

> With this Report, the Commission calls on companies to act now to implement best practices to protect consumers' private information. These best practices include making privacy the "default setting" for commercial data practices and giving consumers greater control over the collection and use of their personal data through simplified choices and increased transparency. *Implementing these best practices will enhance trust and stimulate commerce.*[139]

By repeatedly calling out the danger of poisoning online commerce by failing to adopt practices that respect privacy and engender trust, the FTC was declaring that consumer trust was an important resource that could be destroyed by bad acts by online entities. And by convening regular workshops and issuing reports identifying problems, the agency was encouraging online entities to discuss and, ideally, agree upon ways to avoid that effect.

The FTC's insistence on publicly available privacy policies is notable from this perspective as well. Publicly stated privacy policies make several simultaneous contributions to managing the common-pool resource, i.e., the level of trust. First, all players in the online ecosystem can see them, and thus see what everyone else is committing to.[140] This permits all the major players to see that all the other major players are following the basic rules of the commons. Second, to the extent that consumers know that all major online services *have* privacy policies, this contributes to the level of ambient trust as well.[141] Moreover—and more important—acting under its authority to punish deceptive practices, the FTC took enforcement action against entities who violated their own policies. Online privacy policies thus become credible and enforceable commitments to abide by certain basic rules. These enforcement actions also show consumers that a major federal agency is the

139. *Id.* at i (emphasis added).

140. *See, e.g.*, FAIR INFORMATION PRACTICES, *supra* note 139, at 3-5, 12-19. The FTC's guidance regarding such policies, e.g., that they should incorporate or be based on the FIPs, also aids in this regard, *id.*

141. *Effect of Online Privacy Policies, supra* note 11, at 891.

"cop on the beat" looking out for privacy violations—which, itself, will tend to support trust. Even if consumers do not understand (or care about) the details, to the extent that it is generally known that online entities can get in trouble for privacy violations, consumers will be more confident that significant violations will not occur.

These FTC activities facilitated the creation of a functioning system to manage the common-pool resource of ambient trust. Indeed, its activities have addressed each of the key tasks Ostrom identified as important to developing a sustainable commons:[142]

1. *Define clear group boundaries.* The FTC's exhortations were directed to online entities that collect information about users. These are precisely the entities that constitute the users of the common-pool resource.
2. *Match rules governing use of common goods to local needs and conditions.* Each online entity crafts its own privacy policy, which enables particularized commitments about information collection and usage. At the same time, by convening repeated workshops and issuing reports, the FTC helped articulate how industry should address online trust. Indeed, by helping industry consensus develop, and then relying on that consensus as a basis for taking enforcement action, the FTC ensured that the situation "on the ground" is reflected in the rules.[143]
3. *Ensure that those affected by the rules can participate in modifying the rules.* Online entities can participate both in creating the rules that specifically affect them (their own privacy policies) and those that affect the ecosystem as a whole (by participating in FTC workshops, industry groups, etc.)
4. *Make sure the rule-making rights of community members are respected by outside authorities.* With few exceptions, the FTC has defended self-regulation by the managers of the online ambient trust commons against more stringent legislation or regulations being imposed from the outside.[144] And, the

142. *See supra* text accompanying notes 112-113.

143. *Potential FTC Data Protection, supra* note 34, at 2265 ("The FTC can wait until a consensus around specific standards develops in the industry and then codify them [via enforcement actions] as this happens").

144. There are two notable exceptions. First, in 2000, a majority of FTC Commissioners recommended that Congress pass legislation regarding online data collection and usage. *See* FAIR INFORMATION PRACTICES, *supra* note 139 at 36-37. Second, in 2012 and 2014, the FTC urged Congress to enact legislation regulating data brokers. *See* DATA BROKERS, *supra* note 24, at 49-54 (calling for legislation and noting earlier effort). No legislation resulted in either case. One interpretation is that in calling for legislation, the FTC was signaling to the commons managers that a political problem would develop if the issue were not addressed internally.

FTC reacted extremely negatively when the *FCC* (in 2016) arrogated to itself the task of imposing mandatory privacy obligations on providers of broadband internet access. At that time, the FTC cooperated with industry in a successful effort to have Congress invoke the seldom-used Congressional Review Act to invalidate the FCC's regulations.[145]

5. *Develop a system, carried out by community members, for monitoring members' behavior.* Publicly available sources do not reveal how frequently online entities monitor each other and report abuses to the FTC. That said, the agency certainly monitors online behavior in response to complaints or press reports of claimed abuses. In addition, the FTC's two decades of enforcement actions have contributed to the professionalization of the field of privacy compliance, with the role of "Chief Privacy Officer" now quite common for online entities of any size.[146] This allows for active self-monitoring by dedicated in-house privacy professionals throughout the online economic ecosystem.

---

145. 5 U.S.C. §§ 801-808 (2016). The question of privacy obligations of broadband ISPs arose within the broader dispute over "network neutrality." In order to impose "neutrality" obligations on broadband ISPs, the FCC determined that such entities would be classified as "telecommunications carriers" under the Communications Act. *See* Report and Order on Remand, Declaratory Ruling, and Order, *In re* Protecting and Promoting the Open Internet, 30 FCC Rcd. 5601 (2015), *aff'd sub nom* United States Tel. Ass'n v. Fed. Comm'cns Comm., 825 F.3d 674 (D.C. Cir. 2016) (see discussion of subsequent history below). The FTC's enabling statute, however, removes carriers from the FTC's jurisdiction. 15 U.S.C. § 45(a)(1), (2). *See* Fed. Trade Comm'n v. AT&T Mobility, LLC, 883 F.3d 848, 863-64 (9th Cir. 2018). So, the FCC's classifying those entities as carriers removed them from the FTC's purview. *See* Report and Order, *In re* Protecting the Privacy of Customers of Broadband and Other Telecomms. Servs., 31 FCC Rcd. 13911, ¶ 26 (2016) (noting that prior to classification of broadband as a telecommunications service, privacy issues regarding broadband were subject to FTC authority). With the change of administration in 2017, the new FCC promptly disclaimed—and suspended the operation of—those privacy rules, Order Granting Stay Petition in Part, *In re* Protecting the Privacy of Customers of Broadband and Other Telecomms. Servs., 32 FCC Rcd. 1793, ¶¶ 7-20 (2017), and the Chairmen of the FCC and FTC issued a "joint statement" indicating that the *FTC* was the appropriate agency for handling online privacy issues, Press Release, FTC Chairman Maureen K. Ohlhausen & FCC Chairman Ajit Pai, Joint Statement of Acting FTC Chairman Maureen K. Ohlhausen and FCC Chairman Ajit Pai on Protecting Americans' Online Privacy (Mar. 1, 2017), https://perma.cc/WJP4-W5NH. Congress then invoked the "Congressional disapproval procedure" in the Congressional Review Act, 5 U.S.C. § 802, to invalidate the *FCC's* privacy rules. S.J. Res. 34, 115th Cong. (as signed by President, Apr. 3, 2017), https://perma.cc/5J23-92MN. Finally, the FCC recanted its ruling classifying broadband internet access providers as carriers. Declaratory Ruling, Report and Order, and Order, *In re* Restoring Internet Freedom, 33 FCC Rcd. 311, ¶¶ 20-64 (2018). As of this writing, the FCC's decision to recant its classification of broadband internet access as a telecommunications service is on appeal at the D.C. Circuit. *See* Mozilla Corp. v. FCC, Nos. 18-1051 et al. (D.C. Cir. appeal docketed Feb. 22, 2018).

146. Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground,* 63 STAN. L. REV. 247, 251, 258, 311-12 (2010); *New Common Law of Privacy, supra* note 38, at 585, 606, 616-17, 672 (discussing FTC requirements that firms subject to consent decrees establish

6. *Use graduated sanctions for rule violators.* It is hard to know how well "graduated sanctions" are applied. On the one hand, different infractions have resulted in different sanctions being included in consent decrees.[147] Even so, Professors Hartzog and Solove argue that the FTC could do a better job calibrating its sanctions to different levels of culpability of entities that violate privacy norms.[148] On the other hand, there is no readily available public source of information about informal inquiries by the agency to entities engaging in potential privacy policy violations, which—if the consultations are occurring—could lead to changes in how the firms in the commons handle privacy and trust-related issues that do not rise to the level of formal consent decrees.
7. *Provide accessible, low-cost means for dispute resolution.* The FTC staff is available to members of the online economic ecosystem for discussion regarding whether any particular data collection or usage activities would raise regulatory eyebrows.[149]
8. *Build responsibility for governing the common resource in nested tiers from the lowest level up to the entire interconnected system.* The FTC has encouraged online entities to adopt privacy policies, enabling intra-entity responsibility. The FTC has also encouraged (and, in cases of consent decrees, required) online entities to arrange for third-party audits of compliance,[150] thus providing another tier of review.[151] The ongoing professionalization of the privacy field[152] also reflects the internalization of the process of identifying privacy issues and encouraging compliance with industry norms.

---

internal privacy compliance programs).

147. *New Common Law of Privacy, supra* note 38, at 606-27 (discussing various consent decrees).

148. *Potential FTC Data Protection, supra* note 34, at 2297-98.

149. *See* Consolidated Edison Co. v. Federal Power Comm., 512 F.2d 1332, 1341 (D.C. Cir. 1975) (noting that "[r]egulation through 'raised eyebrow' techniques seems inherent in the structure of most administrative agencies").

150. *New Common Law of Privacy, supra* note 38, at 585, 606, 616-17, 672 (discussing FTC requirements that firms subject to consent decrees establish internal privacy compliance programs).

151. There is some evidence that these efforts have worked to improve online firms' awareness of and compliance with basic privacy obligations. *See* Bamberger & Mulligan, *supra* note 148, at 251, 262-63

152. *See id.*

These FTC actions illustrate that online consumer privacy issues have been managed by a commons, not optimized by a market. The evolution of industry practices regarding online consumer privacy, therefore, has certainly been a form of *economic* behavior. But it has not, fundamentally, been a form of *market-based* behavior.

D. Two Distinctive Features of the Ambient Trust Commons

Two features of trust as a common-pool resource distinguish the ambient trust commons from a more typical commons devoted to managing a physical common-pool resource like a field or a fishery.[153]

First is the nature of the common-pool resource. In most cases, the resource itself—fish in a fishery, grass on a meadow—is not particularly interesting. Instead, the question is the social and institutional rules established to ensure that the common-pool resource is not overused. In the ambient trust commons, however, while the institutional arrangements matter, the details of managing the resource are also critical. This is because, in a fundamental sense, the resource is *us.* What is being managed is *our* level of trust, *our* privacy, and (subject to the Coasian qualifications noted above) *our* information. As citizens and consumers, we have legitimate interests—privacy interests, economic interests, personal interests—that are distinct from the interests of the entities that make use of our trust by surveilling us, profiling us, serving us ads, and selling us stuff. It is doubtless true that in some philosophical sense fish don't want to be fished, but they do not have any direct political or legal voice to protect their interest in being left alone.[154] In a typical commons, the common-pool resource needs to be *managed*, but it doesn't have *political rights.* In the ambient trust commons, by contrast, the resource has not only rights, but also some measure of power to protect its interests.[155]

The second distinctive feature of the online ambient trust commons is the subjective nature of trust. In a natural resource commons, the state of the common-

153. As discussed in Part IV, *infra*, these distinctive features create both problems and potential solutions that might not fit within the standard approaches to dealing with common-pool resource issues. *Cf.* Hirsch, *supra* note 64, at 90-93; *Rethinking Environmental Controls, supra* note 109, at 31-38 (discussing strategies for managing a common-pool resource: exclude new users; set rules for how to use it; and convert it to a property right).

154. Some pro-environmental rhetoric does speak of assigning "rights" to the environment as a whole, or to aspects of it. *See, e.g.*, CHRISTOPHER D. STONE, SHOULD TREES HAVE STANDING? 1-31 (3d ed. 2010).

155. *See, e.g.*, note 36, *supra* (new state laws addressing collection and use of consumer information by online entities).

pool resource is an objective fact—there are only so many fish, only so much grassland, etc. But ambient trust is not a physical quantity whose extent is determined by objective facts. How much trust citizens have in the online ecosystem at any given time—and thus how that trust affects online behavior—is based on what citizens know about how online entities are collecting and using information, and to what ends. One cannot protect a fishery from collapse by keeping the fish in the dark about how many of their number are being taken. In the online ecosystem, however, the trust resource will remain in place as long as the nature and extent of surveillance, what happens with the data thus gained, etc., remain obscure. For managers of the online ambient trust commons, security by obscurity may not work forever—serious breaches of trust are eventually revealed—but it may work for a very long time. From this perspective, consumers may be generally aware that their online activities are far from "private," but that does not mean they have any subjective understanding, for example, of how that information is made available to or used by data brokers and advertisers, or what those entities do with it. The largely subjective nature of the ambient trust resource means that the individual and collective interest of the managers of the commons is advanced by being, at best, vague about what information they gather, how they gather it, and what they and their advertising partners do with it.[156]

IV. MANAGING THE COMMONS

The discussion above establishes a framework for understanding privacy in the online economic ecosystem:

1. Privacy is not a commodity to be bargained over in a market. People aren't good at engaging in that kind of bargaining; no such bargaining occurs in fact; and it's not clear, from the perspective of economics or markets, why the rights in information arising from interactions between an individual and an online entity belong to the individual (to be bargained over) and not the entity (to be exploited at will).
2. Treating privacy as arising from relationships of trust is truer to what motivates privacy concerns than a commodity-based, market-based model.

156. *The Internet's Most Popular Price, supra* note 52, at 641. *Cf. Offer You Cannot Refuse, supra* note 24, at 291-93.

People share information when they trust those with whom they are sharing, and conceal things, to the extent they can, from those they do not trust. If trust proves warranted, it grows; if it is betrayed, it diminishes.

3. Entities in the online ecosystem want to maintain ambient trust so that people keep coming online, sharing information, being surveilled, viewing ads, and buying things. At the same time, those entities make money by making use of trust—by permitting information they gain to be used by third parties who want to get people to buy things they may not really want or need, at individualized prices rather than generally available competitive prices.
4. As a result, online ambient trust (and privacy) is best viewed as a common-pool resource for the online ecosystem, not as a commodity exchanged in a market. Online entities can keep using it as long as they manage it properly, *i.e.,* as long as they ensure the use is not so intense as to cause trust to collapse.
5. Online entities face the same challenges in establishing and maintaining the ambient trust commons as do those setting up a natural resource commons: agreeing on rules for using the resource, ensuring commitment to follow those rules, punishing cheaters, etc.
6. These organizational tasks have been accomplished with the help of the FTC.
7. The ambient trust commons has two unique features that distinguish it from a traditional natural resource commons. First, ambient trust may be used without diminishing its level if the extent and nature of the use is not known—as if a population of fish would not decline if the fish didn't know they were being fished. Second, not only the resource managers, but also the resource—us—has some political power to cause its rights to be protected.

This perspective raises three sets of issues. Part IV.A. brings the perspective of management of a common-pool resource to the familiar issues of targeted advertisements, data breaches, and privacy policies. Part IV.B. considers three aspects of the online trust commons where conflicts between the managers and the resource are most severe: excessive numbers of intrusive ads; price discrimination; and the manipulative side of targeted ads. Excessive and intrusive ads reflect a *failure* of commons management, and a growing response—the widespread use of ad blockers—illustrates the independent agency of the resource. Price discrimination and

manipulative targeted ads are intended to transfer wealth from consumers to producers, in a manner beyond what has typically occurred in the mass market consumer economy. Finally, Part IV.C suggests some ways to address these issues within the framework of existing law.

A. Avoiding Collapse

A key goal of every commons is to avoid collapse of the shared common-pool resource. In the ambient trust commons, nobody wants the dystopia of collapsed ambient trust. This subpart addresses three areas where that agreement seems reasonably robust.

1. Targeted Ads I—Lowering Transaction Costs

The basic idea of ad targeting is a win-win for both consumers and sellers. People's interests, tastes, and budgets differ. To the extent that people can avoid seeing ads for things in which they have no interest, and instead see ads for things they might want to buy, everybody benefits. Even when the consumer doesn't buy at any one time, she learns what products are available, from which vendors, and in what price ranges, making later purchases easier and more efficient. For their part, advertisers don't want to waste money showing music editing software to non-musicians, or showing hiking boots to couch potatoes. It is both to consumers' and sellers' advantage to find a way to provide relevant information.[157]

From this perspective, the online economic ecosystem is a clear improvement over the earlier world of mass media, where a lot of advertising expenditure is wasted, precisely because it can't be targeted. For example, ads for gutter cleaning, men's dress shirts, smoking cessation treatments, and vinyl home siding appeared

157. David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy,* 23 J. ECON. PERSPECTIVES 37, 42-43 (Summer 2009). This is the basic idea of the "attention economy." Herbert Simon captured the trade-off nicely: "[i]n an information-rich world, the wealth of information means a dearth of something else: a scarcity of whatever it is that information consumes. What information consumes is rather obvious: it consumes the attention of its recipients. Hence a wealth of information creates a poverty of attention and a need to allocate that attention efficiently among the overabundance of information sources that might consume it." Herbert A. Simon, *Designing Organizations for an Information-Rich World, in* COMPUTERS, COMMUNICATION, AND THE PUBLIC INTEREST 37, 40-41 (Martin Greenberger ed., 1971). In the attention economy, attention is like money—each person has a limited amount that she must allocate to its best use, and targeted ads help avoid wasted attention. For more detailed treatment of an economy based on scarce attention, see generally TIM WU, THE ATTENTION MERCHANTS (2016); JAMES G. WEBSTER, THE MARKETPLACE OF ATTENTION: HOW AUDIENCES TAKE SHAPE IN A DIGITAL AGE (2014)

in the same publication, directed to the same people, on the same day.[158] From a seller's perspective, one of the key benefits of mass media is their broad reach, which is useful for "brand" or "image" advertising not intended to drive any specific sale to any specific consumer.[159] But that same breadth makes mass advertising imprecise, meaning that lots of people see lots of ads for things in which they have no interest.[160] In traditional media, targeting is only possible on a gross level—ads for eye shadow are more likely to appear in *Vogue* than in *Field & Stream*. As consumers are increasingly subject to a glut of information, the ability to target information to specific consumers who are likely to be interested in a product is a godsend.

One reservation to note: if targeted ads are perceived to be based on the use of, or to reveal, particularly sensitive information, people can react negatively. For this reason, among others, the FTC's guidelines for online behavioral advertising state that firms should not collect particularly sensitive information without affirmative, opt-in consent.[161] Avoiding the use of sensitive information in developing profiles, however, does not necessarily avoid the problem of creepiness. The classic example is the teenager who was identified as being pregnant—and thus a good candidate for ads for baby products—without ever having directly revealed that information to either the store or her father.[162] This shows that sensitive *conclusions* can be mined from *data* that is not particularly sensitive, and illustrates that people are not well-equipped to assess what they might be getting into when they formally or informally "consent" to being surveilled and having information about them mined and analyzed.[163] All that said, the pregnant-teenager incident illustrates not that targeted ads aren't valuable to consumers—she *was* pregnant, after all, and so *would* need baby products—but that advertisers must avoid creating negative feelings with the ads they choose to deploy. That is true, though, of any advertisement. Ads on

158. Ads for those products all appeared in the "A" Section of the June 6, 2018, print version of the *Washington Post*. WASH. POST, June 6, 2018, at A1-A22.

159. Evans, *supra* note 161, at 51 (noting that precise, targeted ads are not useful for brand advertising, "which is generally aimed at a broad audience to influence their views on a company or a product rather than to make a direct sale").

160. The standard quote on this point, often attributed to department store magnate John Wanamaker, states: "Half the money I spend on advertising is wasted; the trouble is I don't know which half." *See, e.g.*, *John Wanamaker*, WIKIPEDIA, https://perma.cc/N858-8UDL (archived Oct. 17, 2018).

161. SELF-REGULATORY PRINCIPLES, *supra* note 25, at 47.

162. Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012), https://perma.cc/2WNS-BNCM.

163. *See also Behavioral Advertising Literature Review, supra* note 52, at 365-66 (people have negative responses to higher levels of personalization in ads).

traditional television broadcasts, for example, must meet standards of good taste in order to avoid offending people. The dangers of giving offense with more targeted and individualized ads become similarly more targeted and individualized, but this is not a new problem, and online advertisers will be highly motivated to keep this from happening.

So, while targeted ads can be problematic in several ways, they have real benefits on which advertisers and consumers both agree. Done right, targeting avoids wasting people's time and advertisers' money by providing useful information about the price, quality, and availability of things consumers want.

2. Avoiding Data Breaches

Another area of high-level agreement between consumers and the online ecosystem is the need to avoid data breaches. Consumers do not want to be exposed to embarrassment, anxiety, or financial harm arising from exposure of information about them (for example, by means of identity theft).[164] The managers of the ambient trust commons agree that data breaches should be avoided, but for different reasons. Online entities know that the more consumers perceive it to be likely that subjectively embarrassing or otherwise damaging information might be disclosed, the less trust they will have and the less they will be willing to share. As a result, there is no dispute over the basic idea that those who hold personal information should take care to keep it confidential via data security measures, de-identification, etc.

The differing interests of consumers and online entities, however, bubble right below the surface. From the consumers' perspective, to use Richards & Hartzog's terms, the obligation of online entities to protect consumers' data follows from the duties of *discretion* and *loyalty* to which those entities become subject as part of their trust-based relationship with consumers. Online firms' incentive, however, is to prevent consumers from *feeling* betrayed, and thus withdrawing from the ecosystem. They do not care, *per se,* that a consumer may be harmed by a revelation of information, and, in fact, they likely doubt that she is.[165] Online firms' efforts to avoid data breaches, therefore, do not constitute an acknowledgement that compensation is appropriate when one occurs. From the perspective of the managers of

164. *Risk and Anxiety, supra* note 55 at 741-43.

165. On the whole, courts share in this doubt, routinely dismissing lawsuits based on data breaches on the ground that merely having one's data exposed or stolen does not constitute sufficient harm to support liability. *See id.*

the ambient trust commons, a data breach is problematic because it harms *them*—by eroding trust—not because it harms consumers. A profile indicating that someone is likely to be interested in hiking boots remains fully effective in targeting ads even if it has been exposed to third parties; an HIV-positive patient will still need her medications, counseling, and other treatments if her status is revealed; and we'll all still use credit cards (albeit with new numbers) if our accounts are compromised.

This difference of perspective explains the seeming inconsistency between companies' executives expressing contrition over data breaches, even as those entities fight (largely successfully) any argument that would impose monetary liability when breaches occur. Again, firms in the online ecosystem are motivated to prevent data breaches, but not because they care about protecting consumers' information—corporations are not people, and thus do not "care" about anything. Instead, they will try to prevent data breaches because public awareness of data breaches erode trust, which harms *them*. They want to avoid breaches—and their human representatives express contrition—to manage consumers' emotional state.

This disconnect between the motivations of consumers and firms in the online ecosystem explains the purpose of, and need for, data breach notification statutes. From an economic perspective, what matters to the online ecosystem isn't that data about a consumer has been exposed; what matters is how the consumer reacts when she *learns* that it has been exposed. Thus, online entities care about publicity surrounding data breaches, because that publicity erodes trust. If that publicity could be avoided, the economic interests of online entities would be unaffected.[166] By contrast, consumers whose data has been breached may well want to alter their behavior—from changing where they shop online to buying credit protection services—based on that information. Hence, states have enacted data breach notification laws—which impose significant obligations on entities subject to breaches—to protect consumers in ways the online ecosystem has no natural, intrinsic reason to do.[167]

166. For an illustration of how the incentives on online entities can be problematic, see Brian Fung, *Uber Reaches $148 Million Settlement Over Its 2016 Data Breach, Which Affected Fifty-Seven Million Globally,* WASH. POST (Sept. 26, 2018), https://perma.cc/J942-325A (discussing settlement arising from claims that Uber failed to disclose data breach in accordance with its obligations under various state statutes).

167. Under some data breach notification laws, notification is required if an unauthorized third party acquires the information, no matter what they might do with it. *E.g.*, CAL. CIV. CODE § 1798.82 (West 2017) (notification requirements apply if "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person"). Other states permit the entity whose systems were compromised to assess the likelihood of actual misuse of the data before requiring notification. *E.g.*, FLA. STAT. § 501.171 (West 2014) (requiring no notice

Data breach notification laws thus illustrate the operation of both distinctive features of the ambient trust commons. First, the need for breach notification laws in the first place illustrates that what matters is not just a failure, from the consumers' perspective, of online entities to fulfill their trust-based duties (by failing to protect the information), but also consumers' *awareness* of that situation. Second, unlike a typical managed resource, consumers have independent political power that can be deployed to protect against actions by the online ecosystem that harm their interests. Breach notification laws thus represent an example of the managed resource asserting its own interests in a legally binding way as against the managers of the commons.

3. Privacy Policies (and Privacy Theater)

The online economic ecosystem depends on maintaining a baseline level of consumer trust, and consumers are happier in a world where a reasonable level of trust is justified. To that end, for two decades there has been consensus that online entities need to take some steps to protect consumer privacy and to be subject to some sanctions if they fail to do so. The existence of enforceable privacy commitments is the bedrock of the online ambient trust commons. Online entities may not commit to much, but the integrity of the commons depends on their being held to whatever commitments they actually make.

This goal is addressed by privacy policies. Any online entity that collects information is legally obliged to have one.[168] And once a firm has made public representations about what it will do to protect privacy, the FTC (and state attorneys general) can take enforcement action if it doesn't live up to those representations.[169]

---

if "after an investigation and consultation with" relevant officials, the entity "reasonably determines that the breach has not and will not likely result in identify theft or other financial harm to the individuals whose personal information" was disclosed). At the federal level, as of this writing, the only legal obligation to report data breaches arises under the Health Insurance Portability and Affordability Act, Pub. L. 104-191, 110 Stat. 1936 (1996), as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 (2009). *See* 45 C.F.R. §§ 164.402-164.414.

168. *See supra* note 40. While there is no generally applicable United States law that requires privacy policies, California law does and, since essentially every internet site available in the United States is accessible from California, that state's law effectively imposes a nationwide requirement. More recently, the European Union implemented Regulation (EU) 2016/679, commonly referred to as the "General Data Protection Regulation," or "GDPR." This regulation imposes a variety of disclosure and related obligations on any entities that collect information about EU residents.

169. *New Common Law of Privacy, supra* note 38 *passim.*

So far so good—having enforceable privacy commitments benefits both consumers and online firms. But there are several problems (from the consumers' perspective) with privacy policies. First, firms get to decide what their policies say without any meaningful bargaining.[170] Firms can thus manage their exposure to privacy-related sanctions by minimizing their obligations, whether by means of open, direct disclaimers, or obscure language that camouflages what information they will collect and what they will do with it. Second, when an online entity has a "privacy policy," many consumers think that means the entity has committed to protect consumer privacy.[171] Yet fundamentally, this isn't true. The business model of ad-supported online entities effectively requires them to surveil consumers to a degree well beyond what is necessary to directly provide the entity's own content or products, and to share the resulting information (directly or indirectly) with third parties to facilitate the sale of ads.[172] Nor can this problem be solved by additional disclosures about the process of surveillance, profiling, and ad targeting. The process by which specific consumers are targeted with specific ads is complex, technical, algorithmic, and constantly evolving, so it is hard to see what type of meaningful "disclosure" could be presented. Moreover, assuming language could be crafted that explained how and why targeted ads were created, and how and why they work, this could well erode, not enhance, ambient trust and thus push the commons towards collapse.[173] Third, in the absence of a statute protecting specific types

170. As noted above, there are some efforts underway to try to make bargaining possible, at least as a matter of technology. *See supra* note 54.

171. *The Internet's Most Popular Price, supra* note 52, at 641.

172. *See supra* note 48. The situation is different for different online entities, varying with how dependent an entity is on ad revenue. While entities whose business models are not heavily dependent on ads can still add to profits by collecting information about their users and selling it (directly or indirectly) to third-party advertisers, their economic motivations for collecting information are both less intense than and, perhaps, qualitatively different from, sites and services that are purely or largely ad-dependent. *See infra* note 220.

173. That said, studies show that when people are given an explanation of what information is being collected, and why it is being collected, they trust the company more than in the absence of such explanations. *See Behavioral Advertising Literature Review, supra* note 52, at 367-68; *Effect of Online Privacy Policies, supra* note 11, at 890-91. A cynic might note that—since people have no way of auditing whether any such explanations are *true*—explanations increase trust in the online business irrespective of what the business actually does. Studies also show that people become more concerned and suspicious when advised that information regarding their online activities is being collected by and/or sold to third parties (*i.e.,* entities other than the online site or service the consumer thinks of herself as visiting). *Behavioral Advertising Literature Review, supra* note 52, at 369-70.

of data, courts are reluctant to view data beaches or misuse of otherwise non-sensitive data as constituting cognizable, redressable injury.[174] The difficulty of achieving individual redress in court is offset, to some extent, by the availability of regulatory sanctions. But regulators are subject to resource constraints and shifting political enforcement priorities, so consumers can't count on regulatory help except in the most egregious cases.[175]

Like data breach notification statutes, therefore, privacy policies, too, illustrate the subjective nature of the ambient trust resource: as long as consumers do not understand that their privacy is not being protected by online firms' privacy policies, they will behave as though it is. As a result, it is in the interest of the online ecosystem to keep those facts as obscure as possible: the more consumers understand them, the lower the level of ambient trust, which will tend to limit online activity and may even push the system towards collapse.[176] While privacy policies are far from useless, ultimately their critical function from the perspective of consumers may be "privacy theater"—something that makes people feel that their privacy is being protected without necessarily protecting it.[177]

B. Conflicts in the Commons

Areas of consensus cannot disguise the conflicts between consumers and online entities about the informational rules of online commerce. In the information warfare of the market, sellers want buyers to buy stuff at high prices and will use all available data to achieve that end. Buyers want to buy some things but not others, and want to pay the lowest prices possible—and need information about product availability, features, and prices in order to effect those desires. The desires of buyers and sellers overlap, so these market conflicts are not some existential Manichaean deathmatch.[178] But the question remains how the managers of the ambient

174. *Risk and Anxiety, supra* note 55, at 738-43.

175. *Digital Market Manipulation, supra* note 27, at 1043 ("The FTC has limited resources and reliably pursues complaints only against very bad or very big players"); *Potential FTC Data Protection, supra* note 34, at 2292-93.

176. While Professor Hirsch recognizes that "if trust absorbs too many body blows, it can crash," Hirsch, *supra* note 63, at 84, he believes that we are not yet near collapse of the ambient trust resource, *id.* at 90-93. I am not so sure. *See infra* notes 191 and 222, and *supra* text accompanying note 106.

177. This term is a nod to Bruce Schneier's concept of "security theater," which "refers to security measures that make people feel more secure without doing anything to actually improve their security." Bruce Schneier, *Beyond Security Theater*, SCHNEIER ON SECURITY (Nov. 2009) https://perma.cc/635F-K2HE.

178. *Digital Market Manipulation , supra* note 27, at 1022 ("Firms have incentives to look for

trust commons use the unique and wildly asymmetric information environment of the online economic ecosystem to their advantage, and how their actions affect consumer and societal welfare.[179] While functioning markets balance and optimize producer and consumer interests, even functioning commons—and certainly a tragic one—may well fail to do so.[180]

Three factors are important. First, sellers know a lot more than they used to about how people decide to buy, including a better understanding of consumers' cognitive limitations and biases (i.e., behavioral economics), and how their brains process information during a decision to buy (i.e., neuroeconomics).[181] The key take-away is that a rational assessment of products' merits and demerits appears to play a smaller role than one might want or suspect. Second, sellers know a lot more than they did in the past about each consumer, individually. This lets sellers personalize their pitches—the point of all the surveillance, data mining, and data brokering discussed above. Third, the rise of the consumer internet gives sellers innumerable opportunities to put their enhanced understanding to work. In the past, there was a clear division between when someone was in the market (say, at the mall) and when she was withdrawn from it (say, taking a walk). Today, people aren't always in the souk, but any time someone is at her computer or smartphone, ads are ubiquitous, and buying is a click away. This lets sellers maximize the chance of selling something, without regard to considerations consumers would bring to the table if they, rather than sellers, chose when and how they would be subject to sales pitches.[182]

---

ways to exploit consumers, but they also have powerful incentives to look for ways to help and delight them").

179. *See id.* at 1004-05 (the online environment gives sellers more options to decide when and how to make pitches to particular consumers).

180. Hsu, *supra* note 132, at 79 ("Whereas [Adam] Smith's lesson is that individuals acting in their self-interest will act to increase collective wealth, Hardin's lesson is that individuals acting in their own self-interest will ruin collective wealth.").

181. *See, e.g.*, Shmuel I. Becher & Yuval Feldman, *Manipulating, Fast and Slow: The Law of Non-Verbal Market Manipulations,* 38 CARDOZO L. REV. 459, 462, 485, 498 (2016) (neuromarketing); *Digital Market Manipulation, supra* note 27, at 1041 (same); Jon D. Hanson & Douglas A. Kysar, *Taking Behavioralism Seriously: The Problem of Market Manipulation,* 74 N.Y.U. L. REV. 630, 637 & *passim* (1999) (behavioral economics); Christine Jolls, Cass R. Sunstein & Richard Thaler, *A Behavioral Approach to Law and Economics,* 50 STAN. L. REV. 1471, 1536 & *passim* (1998) (same).

182. *Digital Market Manipulation, supra* note 27, at 1033 ("It is not clear why firms would ever want to confront the fully autonomous consumer capable of maximizing her own self-interest, potentially at the cost of the firm's bottom line.") (footnote omitted).

Sellers, in short, know better how to tempt consumers, and have more chances to do so. Accomplishing consumers' own long-term goals, however, requires resisting temptation, not succumbing to it.[183] From this perspective, the key conflict between the managers of the ambient trust commons and the common-pool resource (consumers) is the degree to which consumers can control the terms on which online commerce—and thus online temptation—occurs.[184] The remainder of this Part discusses three areas where these conflicts between the managed resource and the managers of the commons are particularly evident and acute:

1. *Excessive and intrusive ads*. While not all commons are tragic, online entities—notably ad-supported websites and services—have faced a specific form of the "tragedy of the commons" with respect to the number and intrusiveness of the ads on their sites.
2. *Price discrimination.* Consumers want the lowest price for whatever they buy—an interest served by competitive markets, where fear of losing customers forces sellers to reveal their best price. Sellers, by contrast, want to extract as much as possible from each consumer on each sale—that is, to engage in as perfect a form of price discrimination as they can manage. Price discrimination is easier in the online marketplace, and that change—made possible by using the data garnered from pervasive surveillance—harms consumers.
3. *Manipulative targeted ads.* If consumers were perfectly rational economic actors, they would budget, avoid buying on impulse, and carefully compare options. Sellers don't want consumers to do those things. Sellers want consumers to buy *their* products *right now*. A key point of targeted ads and profile-based predictive marketing is precisely to interfere with consumers' ability to make calm, careful, rational purchasing decisions.

Each of these situations reflects a conflict that has the potential to degrade ambient trust and destabilize the commons. Each is therefore worthy of special attention.

---

183. In behavioral economics jargon, succumbing to temptation or lacking self-control is referred to as "hyperbolic discounting," which means giving insufficient weight to ("discounting") deferred or longer-term satisfactions. *See Behavioral Law and Economics*, *supra* note 51, at 1043-44.

184. It is telling that some of the people who are most knowledgeable about the psychology of online activity have taken affirmative steps to withdraw from the online world, especially ad-supported social media services like Facebook and Twitter. *See, e.g.*, Paul Lewis, *'Our Minds Can Be Hijacked': Tech Insiders Who Fear A Smartphone Dystopia*, THE GUARDIAN (Oct. 6, 2017), https://perma.cc/U37F-J3WK.

1. The Tragedy of the Ad Commons

One particularly souk-like aspect of the online environment is the number and intrusiveness of ads which online services present. People are not inherently harmed by, or opposed to giving attention to, any one ad. The problem is that each ad-supported online service faces a tragedy of the commons with respect to how many ads to present. Up to a very high limit, no online service has a reason not to display "just" one more ad, or to employ annoying and intrusive formats such as pop-ups, automatic playing of videos, requiring watching ads before the desired content is made available, etc.[185] Within Richards & Hartzog's taxonomy, bombarding consumers with ads breaches the online entities' duties of *protection* and *loyalty*. Instead of being shielded from this unpleasantness, the online entities that consumers need to trust subject them to it.

In a normal tragedy of the commons, one watches in horror as the fishery is depleted or the meadow turns to mud. But in the online ambient trust commons, consumers have agency and the ability to respond. Consumers can use ad blockers to protect themselves.[186] Ad blockers are plug-in programs grafted onto web browsers that recognize ads and prevent them from being displayed. Examples include software such as Ghostery[187] and the Electronic Frontier Foundation's Privacy Badger.[188] Within the framework of the commons, consumers deploying ad blockers represent the resource protecting itself from the managers—the fish fighting back.[189]

Online entities claim that using ad blockers violates consumers' end of the bargain of the web—free content in exchange for viewing ads and providing information (by being surveilled).[190] But people may never have understood that bargain,

185. *See* ANDREW ESSEX, THE END OF ADVERTISING: WHY IT HAD TO DIE, AND THE CREATIVE RESURRECTION TO COME 133 (Kindle ed. 2017) [hereinafter END OF ADVERTISING] ("[E]xasperation is truly the appropriate response to banner ads. It's even harder to imagine anyone celebrating . . . the pre-roll ad[,] the only format in advertising history so neurotically self-aware of its own annoyingness that it provides a countdown to when it can be skipped.").

186. The use of ad blockers is accelerating, with a penetration of approximately 20% of the United States online market. *See, e.g.*, Matthew Cortland, *The State of the Blocked Web: 2017 Global Adblock Report*, PAGEFAIR (Feb. 1, 2017), https://perma.cc/J2AC-CBNP.

187. GHOSTERY, https://perma.cc/CWK2-P7RX (archived Nov. 18, 2018).

188. *Privacy Badger*, ELECTRONIC FRONTIER FOUNDATION, https://perma.cc/4YQ6-S269 (archived Nov. 18, 2018).

189. *Cf.* JAWS (Universal Pictures 1975), https://perma.cc/ED68-VTWM.

190. *E.g.*, Matthew Ingram, *You Shouldn't Feel Bad About Using An Ad Blocker, And Here's Why*, FORTUNE (Sept. 17, 2015), https://perma.cc/GZ5T-9YLA; Interactive Advertising Bureau, *IAB Believes Ad Blocking Is Wrong*, IAB, https://perma.cc/7KDK-AVDZ (archived Nov. 18, 2018).

and even those who acknowledge it in broad outline certainly never agreed to look at any set number of ads. Since the terms of the bargain have never been negotiated, ad blockers are best seen a negotiating tool. In essence, a consumer deploying an ad blocker is going on strike: "cut down the number of ads, or I won't look at all."[191] Of course, websites and online services have bargaining chips of their own. For example, websites can refuse to make their content available to browsers that are running blockers. Sites can also propose a new deal: "You can view the site without ads, but you have to pay to see it"—that is, you have to subscribe.[192]

It is unclear how this battle will play out in the long term. Note, though, that even if deploying ad blockers is a way for consumers to "stick it to the man," ad blockers do not prevent surveillance and tracking. Even "do not track" systems, however well-intentioned, cannot prevent this from occurring. Among other things, online entities will in most cases necessarily receive the IP address indicating where the consumer is connected to the network, which can provide a good way to identify who is online. In addition, "browser fingerprinting" allows the identification of an individual consumer by analyzing certain information about the consumer's browser software that must be transmitted to the website in order to ensure that it displays properly on the consumer's computer screen.[193] The user's profile can then be used to serve targeted ads to people like her who do not have ad blockers.[194]

The growing use of ad blockers is instructive for several reasons. First, it illustrates how the *agency* of the common-pool resource (us) affects the management of the commons. Second, unlike other privacy-related actions within the online information commons, it is difficult for online entities to conceal the fact that consumers are being subjected to ads—which may also explain why technological tools to fight

191. For more on ad blockers, see Jon T. Abrahamsen, Note, *Ad Blockers, Convenience or Trespass? Click Here to Find Out!,* 2017 U. ILL. J.L. TECH. & POL'Y 487 (2017); Tyler Barbacovi, *Blocking Ad Blockers,* 16 J. MARSHALL REV. INTELL. PROP. L. 272 (2017); Ian C. Butler, Note, *The Ethical and Legal Implications of Ad-Blocking Software,* 49 CONN. L. REV. 689 (2016). Some argue that growing use of ad blockers is an indication that the online world is approaching "peak advertising;" Tim Hwang & Adi Kamar, *The Theory of Peak Advertising and the Future of the Web* (Oct. 9, 2013), https://perma.cc/6BNS-Q5YC.

192. Professor Calo suggests that ad-supported online services should be required to offer a surveillance-free, ad-free subscription option. *Digital Market Manipulation, supra* note 27, at 1047-48. *See infra* text accompanying notes 243-246.

193. *Offer You Cannot Refuse, supra* note 24, at 285; *see also id.* at 281-85.

194. In this sense, ad blockers are akin to exclusionary zoning and "NIMBYism," in which well-to-do citizens arrange for undesirable activities (say, a sewage treatment plant) to be located in distant neighborhoods, even while taking advantage of the activities they keep at bay. *See Rethinking Environmental Controls, supra* note 109, at 33 (defining "the NIMBY syndrome").

ads have come into being.[195] Third, questions regarding the number and intrusiveness of ads on a given site have never been a direct focus of FTC oversight. Perhaps the tragedy of this aspect of the commons is attributable, at least in part, to that absence.

2. Price Discrimination and the Battle for Consumer Surplus

Price discrimination means charging similarly situated customers different prices for the same product.[196] In a competitive market, sellers have no power to do this: each seller is compelled by fear of losing business to offer the lowest possible price, equal to the seller's marginal cost, to all buyers. The fact that competition forces sellers to offer all buyers the lowest possible price is a critical underpinning of the claim that permitting market forces to operate maximizes consumer welfare. When the price of each item reflects the value of the underlying resources used to make it, economy-wide decisions about how much of each product to make automatically reflect the relative costs of, and consumer desires for, each product.[197]

---

195. Advertisers are looking for more better ways to use "native" advertising, where the pitch is seamlessly integrated into whatever content is being purveyed. For example, the brands of cars, computers, and other items used in movies by heroes and villains are hardly random. *See, e.g.,* Katy Kroll, *The Most Egregious Product Placements in Movie & TV History,* ROLLING STONE (June 4, 2013), https://perma.cc/NU9R-WUVW; *see also* END OF ADVERTISING, *supra* note 185, Part 3 (discussing different advertising models, such as native advertising and sponsorship of uninterrupted content). Also note the assumption that the ads themselves are not interesting. Gary S. Becker & Kevin M. Murphy, *A Simple Theory of Advertising as a Good or Bad,* 108 QUART. J. ECON. 941, 961 (1993) [hereinafter *A Simple Theory of Advertising*]. Essex argues that a solution is to make ads themselves sufficiently interesting that we will want to look at them. END OF ADVERTISING, *supra* note 185, Part 3.

196. Price differences that reflect cost differences are not price discrimination in an economic sense. For example, if a seller lowers her costs by selling in bulk, it is not price discrimination to offer volume discounts. The focus here is on price discrimination in the economic sense, *i.e.,* discrimination that is not cost-based. Professor Calo suggests the example of a flower seller who might charge more to a customer who the seller knows just had a fight with a spouse. *Digital Market Manipulation, supra* note 27, at 1023-24.

197. *See supra* note 8 and accompanying text. In the actual economy, "with competitive firms facing downward-sloping demand curves selling differentiated products, equilibrium prices are generally above marginal cost." Joshua D. Wright, *The Antitrust/Consumer Protection Paradox: Two Policies at War with Each Other,* 121 YALE L.J. 2216, 2247 (2012). Economists do not view the model of a competitive market as an achievable state against which the world is found wanting; it is an analytical tool illustrating how forces of supply and demand work and what happens when they don't. Harold Demsetz, *Information and Efficiency: Another Viewpoint,* 12 J.L. & ECON. 1, 1-3 (1969); *Behavioral Law and Economics, supra* note 51, at 1036-37. But policymakers care about microeconomic models because of the claim that letting market forces work maximizes societal well-being. When the real world departs significantly from the perfect competition model—which it does—there is no way to know *a priori* which policies will achieve a "second-best" solution, *i.e.,* one that maximizes well-being given real-world conditions. R.G. Lipsey & Kelvin Lancaster, *The General*

Price discrimination, by contrast, decouples price from the cost of the resources used in making a product and links it instead to the vagaries of what each individual consumer might be willing to pay. This severs the link between marginal cost and price, and simultaneously transfers wealth from consumers to producers. At the same time, when a consumer pays more than marginal cost for a product, she has less money left over to buy other products, which lowers her overall welfare. This prevents the market from efficiently allocating resources.[198]

Using perfect competition as a baseline, sellers would not be able to price discriminate at all. Purchasers would be effectively interchangeable and anonymous, and all would pay the same (marginal-cost-based) price.[199] Using monopoly as a baseline, a seller would use price discrimination to transfer all consumer surplus, from all consumers, to herself. Within the online economic ecosystem, one of the key benefits of detailed profiles of individual consumers is that they permit price discrimination without the seller being a traditional monopoly. This "creates objective privacy harm," in that sellers are using "personal information to extract as much rent as possible from the consumer."[200]

Price discrimination is easier in the online economic ecosystem than in past consumer mass markets in two critical ways. First, sellers have deeper insight into what each consumer, individually, is likely willing to pay.[201] Second, because each

---

Theory of Second Best, 24 REV. ECON. STUD. 11, 11-12 (1956-57); R.G. Lipsey, *Reflections on the General Theory of Second Best at its Golden Jubilee,* 145 INT'L TAX & PUB. FIN. 349, 350, 358-60 (2007). So, while microeconomics can provide heuristics for policy, the disconnect between theory and reality means that it can neither dictate policy results nor invalidate other heuristics based on factors like fairness and common sense. The problem isn't the market model *per se;* it's knowing when to apply it, given its limitations. *See* text at *supra* note 3.

198. For a detailed explanation of the ways consumers are harmed by price discrimination, see generally Ramsi A. Woodcock, *Big Data, Price Discrimination, and Antitrust,* 68 HASTINGS L.J. 1371 (2017). Note that in this context, saving for the future is another "product" competing for the consumer's money. Price discrimination, therefore, also interferes with our ability to save and achieve longer-term goals.

199. *See* Ryan Calo, *Privacy and Markets—A Love Story,* 91 NOTRE DAME L. REV. 649, 665-73 (2015) for a discussion of some ways that excessive knowledge as between buyers and sellers can interfere with the smooth functioning of markets as society has traditionally conceived them.

200. *Digital Market Manipulation, supra* note 27, at 1029. *See generally* Aniko Hannak *et al., Measuring Price Discrimination and Steering on E-commerce Web Sites*, PROCEEDINGS OF THE ACM SIGCOMM INTERNET MEASUREMENT CONFERENCE, IMC. 305 §§ 4.3, 5.2-5.3, 7 (2014), https://perma.cc/WCM3-X48X (finding e-commerce websites use data about operating systems and purchasing history to engage in price discrimination and steer consumers to certain products); Glenn Ellison & Sarah Fisher Ellison, *Search, Obfuscation, and Price Elasticities on the Internet,* 77 ECONOMETRICA 427, 427-28 (2009); Rory Van Loo, *Helping Buyers Beware: The Need for Supervision of Big Retail,* 163 U. PA. L. REV. 1311, 1332-34, 1358 (2015) (discussing online price discrimination and related issues).

201. *Control of User Data, supra* note 26, at 443 ("Advertisers are able to exploit the fact that different people have different maximum prices they are willing to pay, the so-called 'pain point'

consumer can be presented with an individually-tailored ad, it takes extra effort—and may be impossible—to determine whether a price is higher than being offered to others. Whereas in the traditional mass consumer economy sellers had to announce their prices to the world—whether in advertisements on TV, radio, or in print media, or simply on store shelves—in the online souk (just like in a real one), a consumer has no way to know whether the price she is being offered is higher or lower than the price other purchasers got.[202] From the seller's perspective, this means that online commerce—based on the information gleaned from surveilling consumers—presents more opportunities to take advantage of whatever market conditions might exist—information asymmetries, oligopoly, brand loyalty, product differentiation—that give the seller some degree of market power. The improved ability of sellers to price discriminate, based on information gleaned from surveilling our online activities, expands their power to extract consumer surplus, and is thus a direct and tangible form of economic "privacy harm."

One counter-point merits discussion. In some cases, consumers arguably benefit, on balance, from price discrimination. The underlying problem arises in markets where producing the product requires making large up-front investments, after which the cost of any one unit of output is small. Consider a new movie that costs $100,000,000 to produce. Once it's made, it can be streamed via broadband internet connections at a cost per stream—that is, at a marginal cost—of essentially zero. If the studio knew it could only charge a marginal-cost-based price for each viewing—say, $0.05—it would know that it could never recover its investment, and the film would never get made in the first place. Economists have no generally accepted way to deal with this type of problem.[203] If a producer is a regulated utility

after which they will not buy the product").

202. Sellers who price discriminate will voluntarily reveal their actions only when it would help with selling. Customers who receive lower prices may be told they are getting "A special discount, just for you!", but those who pay rack rates hear nothing.

203. Brett M. Frischmann & Christian Hogendorn, *Retrospective: The Marginal Cost Controversy,* 29 J. ECON. PERSPECTIVES 193, 201-04 (2015). *See also* R.H. Coase, *The Theory of Public Utility Pricing and its Application,* 1 BELL J. ECON. & MANAG. SCI. 113, 113-14, 121-24 (1970) (discussing the issue in the context of public utility pricing); In today's economy, the problem is particularly acute with products that embody a high degree of intellectual property, such as music, films, literature, software, drugs, or computer chips. Once the first item is produced, it costs little or nothing to produce additional copies. John F. Duffy, *The Marginal Cost Controversy in Intellectual Property,* 71 U. CHI. L. REV. 37, 38-41 (2004) (noting that the issues underlying pricing and related controversies for patented and copyrighted items parallel those for regulated utilities).

subject to a limitation on its total revenues, in theory consumer welfare is maximized by price discriminating using the "inverse elasticity rule."[204] Under this approach, consumers with highly elastic demand (who will buy a lot less of a service as price increases) get a low price, because otherwise they would not buy at all. On the other hand, those with inelastic demand (who will not reduce the amount they buy very much, even as price rises) are charged higher prices. But sellers in the modern online economic ecosystem are neither price-regulated nor revenue-capped, and there is no reason to conclude that unconstrained price discrimination benefits consumers. Moreover, even in the context of regulated rates, price discrimination is often perceived as simply unfair. There may be a range of acceptable reasons for charging some people less than others (few object to discounts for students or seniors), but charging people more simply because they can pay more—or, at particularly weak moments, are willing to pay more—can be socially and culturally problematic.

Price discrimination arises precisely because of the information asymmetry between buyers and sellers, and is facilitated by pervasive surveillance and associated data mining and profiling. It therefore represents use of information gleaned via consumer trust in a manner that does not benefit consumers. One possible solution would be to require online sellers to disclose how the price offered to each consumer fits in the range of prices at which the item is sold. Consumers could then decide for themselves if the item is worth the offered price, armed with the knowledge of whether it is a good or bad one.[205] For example, a seller could offer its goods at any price it wanted to any individual consumer, but would be required to disclose the full range of prices at which the item was offered to all potential buyers. This or some similar disclosure requirement would directly address the information asymmetry in the online ecosystem.

Finally on this point, one might argue that nobody would pay a "high" price once they knew it was high, but that's not necessarily true. For example, consumers

---

204. W. Bruce Allen, *Ramsey Pricing in the Transportation Industries,* 13 INT'L J. OF TRANSPORT ECON. 293, 295-96, 328-29 (1986) (describing theory of inverse-elasticity pricing and noting practical difficulties of implementing it); William J. Baumol & David F. Bradford, *Optimal Departures from Marginal Cost Pricing,* 60 AM. ECON. REV. 265 267-69 (1970); F.P. Ramsey, *A Contribution to the Theory of Taxation,* 37 ECON. J. (1927) 47, 56-59 (inverse-elasticity applied to taxation).

205. A possible legal basis for such a requirement would be that failing to disclose this information amounts to a form of misleading or deceptive practice. *See* 15 U.S.C. § 45. This approach could also help address concerns over fictitious pricing, in which an offered price is falsely represented as a "discount" off of supposedly higher "regular" prices. *See* David Adam Friedman, *Reconsidering Fictitious Pricing,* 100 MINN. L. REV. 921, 964-70 (2016).

who don't want to be bothered shopping around (that is, to incur the transaction costs of continuing to look for the best price) may be willing to pay more for the convenience of immediate gratification. More fundamentally, many consumers may be "satisficers" (satisfied with a "good enough" result) rather than maximizers (always looking for the best possible deal).[206] But if a significant number of consumers wouldn't buy if they knew the price they were being offered was high as compared to others, that's just another way of saying that price discrimination is only feasible due to consumer ignorance—which hardly commends it as a welfare-enhancing practice.

3. Targeted Ads II —Personalized Predictive Profiling

A particularly subjectively disturbing aspect of modern online commerce is the growing use of personalized ads. Seeing too many ads is annoying, but the assault is not subtle or surreptitious. Paying more than others may hurt our pocketbooks, but it is a familiar harm that anyone who has missed out on a sale understands. But personalized ads—pitches directed specifically to *us,* based on detailed, profiled knowledge of our own desires, fears, and weaknesses—can trigger deep unease. We're not just being bothered, or being taken slightly to the cleaners on price. We're being *manipulated.* And if we realize it, we can react viscerally, with feelings of betrayal, anger, resentment, fear, and even self-loathing as we perceive our own agency and autonomy to have been subverted by stealth.

Precisely because the idea of online, personally targeted ads can stir up emotions, the issue should be analyzed carefully. Two key considerations are (a) how are consumers harmed by such ads? and (b) in what ways is that harm *worse* if the ads are based on information about the consumer gleaned from her participation in the online economic ecosystem?[207]

206. Herbert A. Simon, *Theories of Decision-Making in Economics and Behavioral Science,* 49 AM. ECON. REV. 253, 263-64, 277 (1959).

207. The concern in this subpart is not that targeted ads can be creepy and intrusive. Advertisers will surely learn to generate ads that are not perceived negatively. The focus here is on the effects of advertising that—far from being offensive or creepy—are *particularly persuasive* by virtue of sellers' access to detailed information about individual consumers, arising from surveillance of their online activities.

a. The Trouble with Persuasive Ads

The first question is if, and how, consumers are harmed by ads in general.[208] Economists can have trouble making sense of ads. One of the assumptions underlying the idea of competitive markets is that buyers and sellers have perfect information, so to the extent that the purported point of ads is to supply information, their mere existence is something of a rebuke.[209] In any event, the idea that advertising is mainly intended to supply information is inconsistent with the facts. Over time, the information content of ads (in the sense of factual data) has been going down, being replaced by imagery and emotional content.[210] Apple's iconic "1984" ad, for example, conveyed no discernable *factual* information to prove its claim that (roughly) the new Macintosh computer would support rebellious, colorful creative thinking, versus the monolithic computing options offered by IBM and its clones, whose evil, boring dominance could be dramatically destroyed by getting a Mac.[211] Ads in general, and online ads in particular, have been getting shorter and fuller of imagery, with layout and color choices based on what will make people like and want the product, and ever emptier of facts that a rational buyer might want to consider in making a cool, reasoned assessment of where and how to spend her money.[212]

Clearly, the purpose of modern ads is not to assist consumers in rationally assessing their choices in the market; it is to stimulate interest in the products being advertised.[213] If an advertiser can't make people want her product—an emotional

208. Consumers receive some benefits from some advertising, but the standard assumption is that advertising, viewed on a standalone basis, is a net negative in terms of utility. *See, e.g.*, *A Simple Theory of Advertising*, *supra* note 195, at 961.

209. George J. Stigler & Gary S. Becker, *De Gustibus Non Est Disputandum,* 67 AM. ECON. REV. 76, 85 (1977). ("In the conventional analysis, firms in perfectly competitive markets gain nothing from advertising and thus have no incentive to advertise because they are assumed to be unable to differentiate their products to consumers who have perfect knowledge."). "Product differentiation" refers to convincing consumers that functionally identical products are different and developing consumer loyalty to one brand over another, making it possible for sellers to charge above-marginal-cost prices for functionally identical products.

210. *Regulating Non-Informational Advertisements*, *supra* note 33, at 438-51 (discussing evolution of ads, from mainly informative before the 1920s, to mainly emotive by the 21st Century).

211. 1984 (Apple Inc. broadcast Jan. 22, 1984), http://perma.cc/WF8H-8BUP.

212. *Regulating Non-Informational Advertisements*, *supra* note 33, at 438-51. Precisely because these approaches to selling are effective, all sellers must adopt them or lose out in the marketplace. *See Digital Market Manipulation*, *supra* note 27, at 1001; Hanson & Kysar, *supra* note 181, at 635.

213. It is sometimes claimed that ads change consumer tastes, but a more sophisticated analysis begins with the recognition that consumers don't derive utility from consuming *products,* but rather from using those products, along with the consumer's knowledge and time, to create *experiences* that produce utility. Stigler & Becker, *supra* note 209, at 77. Under this model, consumers buy products to assist in obtaining the experiences they want, and advertising conveys how the

response—all the logic in the world isn't going to sell it. But if she can, then she can count on people's higher cognitive capacity to figure out perfectly good-sounding reasons as to why they should buy it.[214]

Recognizing the fundamentally emotional purpose of ads requires a different economic analysis. One suggestion was provided by Coase, who noted that even if an ad doesn't provide information about a product, using the product itself does: "Any advertisement which induces people to consume a product conveys information, since the act of consumption gives more information about the properties of a product or service than could be done by the advertisement itself. Persuasive advertising is thus also informative."[215] Indeed, when the product is an "experience good," consumers can't assess it without trying it.[216] Still another approach was suggested by Becker and Murphy, who posit that ads, themselves, should be viewed as products which are complementary to the ones they advertise.[217] Either way, in economic terms, persuasive ads shift the cost of learning about the advertised products from the seller to the buyer, as compared to informative ads.[218] That is, a buyer

product can be used as an input to the production of the experiences. From this perspective, even vivid, emotional, non-informational "persuasive" advertising doesn't change tastes; it educates consumers about how to use the product—essentially by illustrating how it might fit into the consumer's actual or imagined life. *See id.* at 83-87.

214. *See generally* JONATHAN HAIDT, THE RIGHTEOUS MIND: WHY GOOD PEOPLE ARE DIVIDED BY POLITICS AND RELIGION ch. 1-4 (2012). Haidt, updating Hume, contends that, if reason isn't exactly a *slave* to the passions, it is their *lawyer*, justifying what people's feeling, emoting selves want to do. *Id.* at ch. 3. This is a slightly different take on the idea of "System 1" thinking (quick, intuitive, heuristic-based) versus "System 2" thinking (careful, deliberative, evidence-based) that Daniel Kahneman elaborates in THINKING FAST AND SLOW. *See generally* DANIEL KAHNEMAN, THINKING FAST AND SLOW ch. 1-9 (2011). Where Kahneman focuses on how we process information and use it to make decisions, Haidt suggests that many (perhaps most) of our decisions are actually "made" by our emotions, with logic and reason cleaning up the resulting mess by explaining the decisions—to ourselves and others. A more nuanced view is that emotions provide "somatic markers" that are applied to mental images of the results of different decisions. The somatic markers—unarticulated but nonetheless experienced emotional responses—then steer people towards or against particular actions. *See* ANTONIO DAMASIO, DESCARTES' ERROR 127-204 (1994).

215. R.H. Coase, *Advertising and Free Speech,* 6 J. LEGAL STUD. 1, 9 (1977).

216. The notion of an "experience good" traces to Phillip Nelson, *Information and Consumer Behavior,* 78 J. POL. ECON. 311 (1970). One way to advertise experience goods is to give out free samples, which a bakery might do to help sell cookies. Note also that, while it may be difficult to cast some truly mundane items as "experience" goods—a bushel of wheat is a bushel of wheat—other items can have experiential overlays on their basic function. Any functional automobile will get me from home to my office, but the perceived experience—both in terms of features (e.g., the quality of the sound system) and in terms of the social, psychic value—will differ if I am driving a 2008 Toyota Prius versus a 2018 Lexus SUV.

217. *A Simple Theory of Advertising, supra* note 195, at 961. Goods are complementary when higher consumption of one leads to higher consumption of the other. Becker & Murphy recognize that treating advertising as a product doesn't mean it has *positive* value to consumers; to the contrary, they assume that in many cases ads have negative value to consumers.

218. Coase was thus being a bit sloppy in suggesting that the *persuasive ads*—which are free

must buy the product first and see if it is what she really wants. That entails taking a risk. Buyers will try to minimize the risk by gaining what information they can, but ultimately, for experience goods, or goods with a non-trivial experience component, buyers just have to buy and see how it goes. Sometimes the buyer will like a product, but other times she won't. She'll certainly know not to buy the product *again,* but, counter-intuitively, she will have *added* to the seller's profits for the privilege of learning she doesn't like it. It follows that whatever else it represents, the shift towards ever-more-persuasive, and ever-less-informational advertising reflects a shift of potentially substantial costs from sellers to consumers.

This analysis provides an economic basis for concern with the trend away from informational advertising and towards persuasive advertising. Put aside concerns about ads debasing our culture, hijacking our autonomy, etc.[219] The shift to persuasive ads simultaneously reflects, embodies, and enables a diffuse, but significant, wealth transfer from consumers as a group to sellers as a group. There may be some offsetting benefit, in the form of slightly lower prices, to those who try products and like them, but on balance, this new arrangement seems likely to be a better deal for sellers than for buyers.

This also provides a basis for being particularly nervous about advertisers applying behavioral economics, neuroeconomics, and other data-based and science-based disciplines in developing persuasive ads. In the absence of thorough and reliable information, the first time a consumer buys a product, she is subjecting herself to the risk that she won't like it. In deploying their understanding of behavioral economics, etc., sellers are doing everything they can to get consumers to take that risk and try the product, at the consumers' expense. In effect, they are selling a meta-product—the idea that consumers ought to try the product itself. It's easy to see why consumers could feel manipulated by this situation.[220]

---

to the consumer—convey information. *Buying and using the product*—decidedly not free—is what conveys the information.

219. For better or worse, America has, and has long had, a culture in which commerce and selling—particularly mass-market commerce and selling—play a prominent role. Objections to the ill effects of advertising on, or the generally prominent role of commerce in, our culture, are of a different order than the issues addressed here. *See supra* note 33.

220. Sellers are, of course, aware of this consumer concern, which has led them to try to assuage it by (at least in some cases) offering no-hassle returns. A no-hassle return policy allows the consumer to think that she'll send back something she doesn't like, while actually establishing a "default" case where the product is in the consumer's hands and thus likely to remain there. Online services which are closer to a theoretically ideal free-to-the-consumer ability to try out "experience" goods are Amazon's Prime Wardrobe, https://perma.cc/X489-RCYU (archived Oct. 27, 2018) and Stitch Fix, https://perma.cc/HZ2E-NC7R (archived Oct. 27, 2018). These services send clothes to consumers to try on, with no charge, and free return shipping, for items not

A potential counter-point is that the vast amount of information available online, in the form of product reviews, recommendations from sites like Yelp! or Angie's List, or indeed the websites of the sellers themselves, fully address consumers' need for information. With that information readily available, it would be wasteful for sellers to spend ad dollars conveying it again. In a gains-from-trade analogy, third-party sites and consumer recommendations have a comparative advantage in providing information, leaving to the sellers the different—but also important—task of stimulating demand, in which *they* have a comparative advantage. There is something to this critique, but it does not undermine the basic point that sellers' interest is in getting consumers to buy the product whether it will actually prove satisfactory or not. Moreover, the greater the portion of a product's utility that resides in subjective experience, the less objective information— from websites or otherwise—would assist in the buying decision.[221]

b. The Trouble with Targeted Persuasive Ads

The discussion above provides a framework for understanding the particular concern about targeted ads based on detailed profiles derived from data-mining information surveilled during a consumer's online activities. In addition to using the data to present the consumer with ads for things that she is likely to want—the good side of targeted ads—sellers will also use the data to ever more effectively get her to take the risk of trying products that might not work for her, at her expense. Targeting ads, based on a consumer's individual characteristics, increases the risk that she

---

selected. As relevant here, note, first, that the fundamental business model of these services is *selling things directly to consumers,* not extracting information from and about them for use by third party advertisers. Using these services is more like choosing to go to the store than being bombarded with ads. Moreover, while these services obviously depend on targeting a consumer's tastes and preferences, the targeting is essentially entirely overt—indeed, it's part of the appeal of the services. That is, they'll learn what clothes the consumer likes and make an effort—which she will appreciate—to only send clothes that will meet with her approval.

221. As style, status, etc. play a larger role in products' value, the portion of utility derived from how the product makes the buyer feel goes up, so more of consumers' expenditures (and well-being) is tied to the social/cultural, as opposed utilitarian, aspects of products. This will increase the degree to which consumers must bear the risk of buying a product to see if the experience of owning it is worth the money. On the other hand, advertising a product a consumer already owns can improve her utility by confirming that the product is valuable in terms of status, style, etc. *See, e.g.*, Len M. Nichols, *Advertising and Economic Welfare,* 75 AM. ECON. REV. 213, 213-14 (1985) (suggesting that owners of a particular brand of tennis racket will obtain increased utility at no additional cost when the manufacturer advertises a new celebrity endorsement for the brand). Advertising these types of products—call them "social experience goods"—is an effort to get new customers to take the risk of buying them, but also a form of ongoing customer support, like free software updates, for those who have already bought.

will buy things that she ultimately doesn't want or like. While online sellers will know not to offer hiking boots to a couch potato, they will also try everything they can to get a hiker to buy an extra pair of boots. This creates the same kinds of economic harm described above, arising from persuasive, non-informational ads in general. The concern is that sellers' efforts to get people to take the risk of trying their products will be even more effective when deployed based on specific information about each individual consumer. This therefore exposes consumers as a group to more risk, and shifts more wealth from consumers to sellers, than persuasive ads in general.[222]

In terms of the ambient trust commons, this adds insult—and maybe even additional injury—to injury. As compared to a baseline of informational ads, when people participate in the online economic ecosystem, they are being pressured and tempted by sellers, presenting scientifically-informed, specifically targeted persuasive ads. Rather than protecting consumers from those pressures and temptations, the online economic ecosystem helps sellers deploy them even more effectively. In Richards & Hartzog's terms, this represents a failure of the duty to protect and be loyal to the consumers who trust online entities with their information and attention.

There is substantial precedent in pre-internet law recognizing that personalized sales pitches can be qualitatively different from more generalized, mass-market advertising.[223] For example, in 1971, the FTC established a rule requiring that consumers who buy something as a result of a direct solicitation in their homes have a 3-day period to cancel the transaction, no questions asked, and get back any money paid as a deposit.[224] The reason for the rule is the common-sense understanding that people are subject to pressures in the direct sales context that do not

222. An extreme form of risk to consumers from ads is fraud. Blogger (and former *Linux Journal* editor) Don Marti suggests that targeted ads inherently lead to an increase in fraud and deception, because deceptive ads can be targeted towards those whose profiles indicate gullibility, and away from enforcers, who would take action if they saw the fraudulent ads. Don Marti, *Simulating a Market with Honest and Deceptive Advertisers,* BLOG: DON MARTI (June 11, 2018), https://perma.cc/63UE-3QVK; Don Marti, *When Can Deceptive Sellers Outbid Honest Sellers for Ad Impressions?,* BLOG: DON MARTI (Apr. 14, 2018), https://perma.cc/F766-KJXJ. *Cf. supra* note 117 (discussing naïve versus predatory "prisoner's dilemma" algorithms). Using a prisoner's dilemma analogy, targeting enhances the ability of predatory "always defect" algorithms (fraudulent sellers) to isolate pockets of naïve "always cooperate" algorithms (gullible buyers) and target them for exploitation.

223. *Information Fiduciaries*, *supra* note 46, at 1217-20.

224. The rule was originally promulgated in 1972. For in-home sales, the minimum amount for the rule to apply is $25. Recently the rule was amended to impose a $130 minimum for out-of-home sales occurring at temporary locations (tents, convention halls, etc.). *See* 16 C.F.R.

arise when the consumer decides for herself when and where to shop. Later, in 1978, the Supreme Court upheld an Ohio bar association rule banning lawyers from directly soliciting clients for contingent fee arrangements in personal injury cases.[225] The Court found that it was reasonable for the bar association to view such arrangements as unfair, both because of the vulnerability of the clients being solicited and because lawyers are "trained in the art of persuasion."[226] In this same vein, in 1985, the Court analyzed the obligation of investment advisors to be registered before giving personalized investment advice.[227] While the First Amendment forbids requiring registration or imposing other obligations on entities that publish investment advice or recommendations to "the general public," there was no First Amendment violation in requiring registration of, and imposing special duties on, entities that provide "personalized" advice.[228]

From the perspective of the online trust commons, the question is whether the degree of personalization made possible by the collection and processing of data from online surveillance rises to the level of special concern illustrated by these precedents. There is no clear answer. An ad on a screen is just an ad on a screen and, as noted above, people ignore the overwhelming majority of them.[229] On the other hand, the vast number of ads to which consumers are subject is intended precisely to catch each consumer at those times when she is vulnerable to temptation, however few and far between such times may be.[230] Moreover, in the situations addressed by the pre-internet cases noted above, consumers always knew that they were being directly and personally pitched, which enabled them to muster what psychological resources they could to resist. In the online economic ecosystem,

§§ 429.0-429.3. Statutory or regulatory rights of rescission exist for certain other selected types of transactions as well. *E.g.*, 15 U.S.C. § 1635 (permitting, under certain conditions, rescission of consumer credit transactions, other than mortgages, establishing a lien on a consumer's home).

225. Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447 (1978).

226. *Id.* at 465.

227. Lowe v. Sec & Exch. Comm'n, 472 U.S. 181 (1985).

228. *Id.* at 206. *See also* Commodity Futures Trading Comm'n v. Varuli, 228 F.3d 94 (2d Cir. 2000); Sec. & Exch. Comm'n v. Gun Soo Oh Pak, 99 F. Supp. 2d 889 (N.D. Ill. 2000); Commodity Futures Trading Comm'n v. Avco Fin. Corp., 28 F. Supp. 2d 104 (S.D.N.Y 1998).

229. *See supra* note 31.

230. The consensus view among psychologists is that people have a limited stock of willpower (the ability to resist temptation) that can be used up by any number of stressful events—including resisting temptation. *See* Roy F. Baumeister, et al., *The Strength Model of Self-Control*, 16 CURRENT DIRECTIONS IN PSYCH. SCI. 351, 351-52 and *passim* (2007). One point of profiling and targeting is to predict which consumers will respond to which ads at which times. But even if these efforts are not fully effective, a constant background barrage of ads maximizes the chance that any given consumer will see at least some ads during periods when her willpower is maximally depleted. *See supra* notes 31-34 and accompanying text.

however, the consumer will not necessarily understand how, or even that, the ads she is seeing have been formulated just for her. This stealth personalization means that the consumer will not be on her guard as she would be in an in-real-life direct sales situation, and so may be more susceptible to the ads.[231]

Ultimately, the concern about targeted ads boils down to two points: (a) we are subject to temptation; and (b) sellers know how to tempt us. This is hardly news. Resisting temptation isn't easy, but it's a challenge people have been dealing with at least since the Garden of Eden (obviously, with mixed success). Part of growing up and being an adult in a market economy means learning how to conduct oneself in the market. And, there seems to be something of a "Flynn Effect" with regard to online advertising—people get better at ignoring it and resisting it as time goes on.[232] Indeed, barring an absolute ban on targeted advertising—which, even putting aside First Amendment problems, would be difficult to police—it is hard to see what could be done to directly alleviate the increased ability of sellers to tempt us. As with being offered discriminatory prices based on individualized profiles, on some level the problem is that people don't know or perceive what's happening. But unlike price discrimination, there is no specific disclosure that would seem to address the issue. Perhaps the best course here would be to accelerate the online Flynn Effect by providing clear and repeated public discussions of how online ad targeting is produced, how and why it works, and mental tricks people can use to arm themselves against it. Forewarned is forearmed.[233]

---

231. *Digital Market Manipulation, supra* note 27, at 1033 ("It is not clear why firms would ever want to confront the fully autonomous consumer capable of maximizing her own self-interest, potentially at the cost of the firm's bottom line") (footnote omitted).

232. Hwang & Kamar, *supra* note 191. The "Flynn Effect" refers to the fact that scores on intelligence tests have been rising consistently for many decades, making it necessary to recalibrate how those tests are scored in order to ensure that the average stays at 100 (or whatever numerical value is set as the average for a particular test). *See, e.g.*, Tamara C. Daley, et al., *IQ on the Rise: The Flynn Effect in Rural Kenyan Children*, 14 PSYCH. SCI. 215 (2003). To the extent that there is a Flynn Effect for online ads, it amplifies the motivation of the managers of the online ambient trust commons to do what they can to keep consumers in the dark about what marketing is going on and how it works, because the better people are at resisting ads, the less advertisers will pay websites and social media services to serve them up. *See also supra* note 191.

233. There may be evidentiary grounds for hope on this front. While many of the cognitive limitations and problems on which behavioral economics is based are readily repeatable in the lab, they do not necessarily appear in real markets, and with proper framing can be reduced or eliminated even in the lab. *See Behavioral Law and Economics, supra* note 51, at 1045-48 (discussing ways of mitigating cognitive biases and limitations). On the other hand, some evidence suggests that knowledge is not necessarily power: "The more people think they know about how [targeted advertising] works … the more they tend to overestimate [its effects] on others and underestimate its effects on themselves." *Behavioral Advertising Literature Review, supra* note 52, at 368. People may all be subject to a version of the Dunning-Krueger Effect in the context of resisting the temptations provided by targeted ads.

C. *Improving the Commons*

Online entities need to ensure that the level of ambient trust doesn't go low enough to cause collapse. At the same time, they make much of their money from activities that, directly or indirectly, take advantage of that trust. This aspect of the online economic ecosystem functions as a commons—with people's trust as the managed common-pool resource—and not as a market. As a result, there is no reason to think that the particular uses of consumer information (and thus of consumer trust) that online entities view as ideal are the same as, or even near to, those that would optimize social welfare in the way that competitive markets are supposed to do—much less the level that consumers would want if they could simply decide the rules.[234]

The discussion above has identified several ways that the current regime may be imposing costs on consumers that would not persist if, somehow, a market could be made to work in this realm. First is price discrimination which, as discussed above, uses differential pricing to shift consumer surplus to sellers—almost by definition an uncompensated loss. Second and third are the "bad" aspects of targeted ads—the fact that they can be used to encourage the purchase of "experience" goods that consumers don't ultimately enjoy, and, more generally, the fact that they can be used to appeal not just to consumers' true preferences for particular products, but also to prey on consumers' increasingly-well-understood weaknesses—essentially, the tendency to buy on impulse (of one or another kind). Fourth is the exposure of consumers to the risk of harm (even if it is often psychological rather than pecuniary in nature) from data breaches. These costs and risks arise by virtue of the availability of detailed profiles of consumers, developed from pervasive online surveillance. Therefore, using Richards & Hartzog's taxonomy, these can reasonably be viewed as "privacy harms" because they arise from a failure of the online ecosystem to fulfill one or more of the duties of honesty, discretion, protection, and loyalty.[235]

In market-based terms, the deal currently on offer is that consumers get free content and services online, and in return, give consent to be surveilled, profiled, subjected to targeted ads, and thus also subjected to the risks and costs identified above. Assume that everything done today with consumer information would still be done, but that we could somehow establish a functioning market to equilibrate the interests of consumers and businesses, leading to some kind of bargained-for

234. *See supra* Part III.

235. *Taking Trust Seriously, supra* note 55, at 459-71.

solution. A consumer would reasonably seek payment from the online ecosystem for several currently uncompensated costs: (1) the costs of paying higher-than-competitive prices due to price discrimination; (2) the costs of buying "experience goods" that turn out not to suit; (3) the lost utility from impulse buying (and thus mis-budgeting and under-saving) arising from being subject to targeting focused on the consumer's susceptibility to temptation rather than her long-range preferences; and (4) the risk of having information exposed due to data breaches.[236]

This hypothetical consumer demand for payment is problematic, but in an instructive way. Even if online entities were willing to pay—which they could at least in theory do as a result of the payments they get from advertisers[237]—how could they know which consumers would be subject to which discriminatory prices, or succumb to which temptations to buy which things at which times? While there certainly are information asymmetries in the online ecosystem, with regard to the question of how much consumers "should" be paid (in the formulation above), the situation is entirely symmetric—both groups are utterly ignorant and, therefore, unable to strike any bargain at all, much less a fair one.

The question is what, if anything, we can or should do about this as a public policy matter.

One option is to do nothing. This would make sense if the harms identified above aren't big enough to be worth doing anything about. It would also make sense if we think the problem will work itself out over time as consumers become more familiar with how online commerce (which is still evolving) works.[238] And, finally, it would make sense if—no matter how big the problem might be—we can't think of anything practical to do.[239] Perhaps we really do have no privacy, and really should just get over it.[240]

---

236. Another way to conceptualize the issue is to borrow Rawls' idea of an "initial position" behind a "veil of ignorance." *See* JOHN RAWLS, A THEORY OF JUSTICE (1971), ch. 3, and especially § 24. One can imagine a discussion between a representative of consumers and a representative of the online ecosystem over these issues, each fully informed of all the facts needed to understand how the online ecosystem works, human decision-making limitations, etc., etc.—*see id.* at 137-38—but unaware of whether they represented the consumers or the ecosystem. In such a situation, they would have no choice but to openly and honestly discuss the operation of the online ecosystem and try to come up with a fair set of rules of engagement.

237. If advertisers wouldn't be willing to pay enough to cover these costs, that would indicate that the practices at issue are a net loss to society.

238. *See supra* notes 232-233 and accompanying text.

239. *Cf. Rethinking Environmental Controls, supra* note 109, at 9, 16-18 (suggesting that doing nothing is a viable strategy when the pressure on the common-pool resource is relatively low).

240. Then-CEO of Sun Microsystems, Scott McNealy, famously said that "consumer privacy issues are a 'red herring.' 'You have zero privacy anyway. . . . Get over it.'" Polly Sprenger, *Sun on*

The idea that the problem of consumer concerns about how their information is used—that is, of trust—will work itself out over time is implausible. The subjective nature of the trust resource means that participants in the online economic ecosystem are subject to a form of "moral hazard"—they will likely make more money if people don't know what's going on. In this regard, recall that even the basic implementation of privacy policies did not come into being due to market forces. They arose from FTC exhortations (as part of its construction of the ambient trust commons) and statutory obligations (imposed by California and thus, as a practical matter, effective everywhere).[241] The prospect that this situation will naturally resolve itself in a manner that optimally balances consumer and producer interests is remote.

So, what might we do?

One option—which seems hard to argue against—is that we should do a better job of educating the public about how behavioral advertising in general, and personalized, targeted behavioral advertising in particular, do their work.[242] Sellers will always try to tempt us, and in a market economy they are entitled to try. But there's no reason to make it easy for them.

Second, to deal specifically with price discrimination, it would not be unreasonable to require sellers to indicate where the price currently on offer to a given customer sits in relation to other prices the seller has made available.[243] This would not constrain what sellers could charge, but it would better inform consumers.[244]

Finally, while it needs some tweaking, there is merit to Professor Calo's suggestion that ad-supported websites and online services be required to offer a no-

Privacy: "Get over it", WIRED (Jan. 26, 1999), https://perma.cc/XJV6-8P4Z.

241. *See supra* Parts II.C. and III.C.

242. This might include the FTC mandating or encouraging that privacy policies make certain disclosures prominently, at the beginning of the document, in large fonts, etc. For the FTC to impose a formal, binding rule on this topic would be a procedural challenge under its existing statute, although it would not be impossible. *See* 15 U.S.C. § 57a (imposing burdensome procedural standards for rulemakings). A more procedurally simple approach might be for the agency to challenge unduly vague privacy policies, on a case-by-case basis, as "deceptive"—even where the affected entity has (at least arguably) abided by them. *Potential FTC Data Protection, supra* note 34, at 2263-64. Even under that approach, however, the agency would do well to develop a robust record demonstrating that consumers do not understand privacy policies as currently drafted, and that consumers would act differently to protect their interests if they did understand the online entities' actual privacy practices, i.e., what actually happened with the data gleaned from surveilling consumers. Of course, states may also have a role to play here. *See supra* note 40.

243. See supra Part IV.B.2.

244. As discussed above, this would not necessarily mean that consumers would never be willing to pay a "high" as opposed to a "discounted" price. *See supra* notes 205-206 and accompanying text.

ads, no-tracking paid subscription option.[245] There's no such thing as a free lunch and, online, there's no such thing as free information, so it's only fair that content providers get paid for what they provide.[246] But there is no reason consumers should have to sacrifice information about themselves (thereby feeding the economic beast of profiling) and subject themselves, and others, to ads they don't want to see, if they are willing to pay directly for the content and online services they want. It is not unreasonable, given the evolution of the online economic ecosystem, to require content providers to offer them that option.[247]

This requirement would constitute direct regulation of online entities, and thus may raise objections from free-market devotees. In fact, however, it is a market-enabling and market-enhancing form of regulation. First, it has the potential to provide a great deal of informative and interesting market data, to consumers, content creators, publishers, and advertisers alike. In addition to having the option of avoiding ads and tracking, consumers would get direct market signals as to how much their information and their eyeballs are worth—as indicated by how much they would have to pay to avoid surrendering access to them. Content creators, in turn, would get direct market signals as to how much their content is worth, effectively directly from those who consume it. That will provide incentives for them to generate more interesting and more valuable content. Similarly, publishers (and social media service providers, etc.) would get direct signals regarding the value to consumers of what they provide, and would thus have incentives to increase that value, whether in terms of the underlying content, the format in which it is presented, or any other variables relevant to consumers.[248] Finally, for perhaps the first time, this

245. *Digital Market Manipulation, supra* note 27, at 1047-48. One potential tweak would be to limit the requirement to sites that meet some minimum size threshold—say, a minimum of 10,000 unique visitors per month. There's no reason to require every blogger with a few ads on her site to have to arrange to take credit cards. Another potential tweak might be to put some upper limit on the price of a subscription—perhaps initially based on some multiple of a site's average per-user advertising revenue—so that it reflects a realistic option.

246. While it is often stated that "information wants to be free," the actual context of the quote (from Stewart Brand) is instructive. In the course of a conversation with Apple's Steve Wozniak about the availability of, and the prices for, software, Brand stated: "On the one hand information wants to be expensive, because it's so valuable. The right information in the right place just changes your life. On the other hand, information wants to be free, because the cost of getting it out is getting lower and lower all the time. So you have these two fighting against each other." *See* Steven Levy, *"Hackers" and "Information Wants to Be Free"*, BACKCHANNEL (Nov. 21, 2014), https://perma.cc/CP3R-YMNU.

247. *See supra* Part IV.B.1.

248. It would also enable online publishers and other service providers to consider the costs they incur in order to facilitate surveillance and the ability to serve up targeted ads. It might turn

arrangement would create a market in which advertisers would have to directly confront the long-recognized fact that in many cases their output, considered on its own, is an uninteresting, annoying intrusion that consumers will avoid if they can.[249] This will provide incentives for advertisers to make their own output interesting, engaging, and informative. Over time, this may even have the effect of shifting back to sellers more of the cost of educating consumers about the features and attractions of products without having to buy them to find out.[250]

V. CONCLUSION

Market forces do not protect consumer privacy interests in the online economic ecosystem. Instead, this ecosystem is best conceived as a commons, in which consumer trust (from which privacy interests arise) is the managed common-pool resource—with online entities, aided by the FTC, acting as the commons managers. The choice of model matters. In the market model of privacy, whatever terms of engagement emerge between consumers and online entities regarding privacy and surveillance come with at least a weak presumption of optimality—that is, that they reflect a fair balancing of consumer and seller interests. In the commons model, however, there is no reason to think that the interests of consumers (whose level of trust is the common-pool resource) are being optimally balanced against those of sellers. Again, the economic objective of the commons managers is not to protect privacy; it is to surveil consumers, and use the data thus gleaned to make it easier to sell things—many of which, of course, consumers want, but others of which they would do better to do without. In this situation, there are some genuine and ongoing conflicts between consumers and the online ecosystem in which consumers increasingly spend time and money, conflicts that we cannot expect market forces to fairly equilibrate or optimize.

In light of all this, we should consider some modest public education and regulatory efforts, outlined above. These proposals would begin both to address the information asymmetry problems and to empower consumers to enjoy online content, and transact business online, without having to sacrifice undue amounts of their privacy or their money.

---

out that online services can make more money—and have happier consumers—using a subscription model as opposed to an ad-supported model.

249. *A Simple Theory of Advertising, supra* note 195, at 961; END OF ADVERTISING, *supra* note 185 *passim.*

250. *See supra* Part IV.B.3.